2013-03

DETERRENCE AND CYBER-WEAPONS

Hemmer, Patrick T.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DETERRENCE AND CYBER-WEAPONS

by

Patrick T. Hemmer

March 2013

Thesis Advisor: Leo Blanken
Second Reader: William Robinette

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE DETERRENCE AND CYBER-WEAPONS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Patrick T. Hemmer			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Rapid technological advancements and societal inclusion of these technologies have expanded civil and defense capabilities but have also created significant vulnerabilities. Cyber-weapons have the potential to affect interaction between states by exploiting this vulnerability. To better understand the mechanics of how cyber-weapons affect state relations this research applies a common framework to explore the attributes of traditional weapons—conventional, nuclear, and RMA—and how they typically influence this behavior. After proposing selected factors that influence the effectiveness of a cyber-attack, the research examines the cyber-attacks in 2007 on Estonia and 2008 on Georgia in order to refine and provide nuanced analysis on the role of the proposed causal factors. The proposed factors are government involvement, level of attack sophistication, and the degree to which the state is dependent upon digitally connected technology. The research indicates that the role of the state is one of the most significant factors in influencing the effectiveness of a cyber-attack and highlights the role that plausible deniability plays in this relationship. Some initial policy recommendations are made based on the finding that the use of cyber-weapons as a deterrent is still ill-defined and that the focus should be on decreasing state vulnerability to these attacks.

14. SUBJECT TERMS Cyber-deterrence, offensive cyber-attacks, Estonian cyber-attacks, Georgian cyber-attacks			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

DETERRENCE AND CYBER-WEAPONS

Patrick T. Hemmer
Major, United States Army
B.S., United States Military Academy, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Patrick T. Hemmer

Approved by: Dr. Leo Blanken
Thesis Advisor

CDR William Robinette
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Rapid technological advancements and societal inclusion of these technologies have expanded civil and defense capabilities but have also created significant vulnerabilities. Cyber-weapons have the potential to affect interaction between states by exploiting this vulnerability. To better understand the mechanics of how cyber-weapons affect state relations this research applies a common framework to explore the attributes of traditional weapons—conventional, nuclear, and RMA—and how they typically influence this behavior. After proposing selected factors that influence the effectiveness of a cyber-attack, the research examines the cyber-attacks in 2007 on Estonia and 2008 on Georgia in order to refine and provide nuanced analysis on the role of the proposed causal factors. The proposed factors are government involvement, level of attack sophistication, and the degree to which the state is dependent upon digitally connected technology. The research indicates that the role of the state is one of the most significant factors in influencing the effectiveness of a cyber-attack and highlights the role that plausible deniability plays in this relationship. Some initial policy recommendations are made based on the finding that the use of cyber-weapons as a deterrent is still ill-defined and that the focus should be on decreasing state vulnerability to these attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- **A. OVERVIEW....1**
- **B. PURPOSE....2**
- **C. RELEVANCE....3**
- **D. THESIS ORGANIZATION....3**

II. FRAMEWORK....5
- **A. BASIC ASSUMPTIONS OF INTERNATIONAL RELATIONS SYSTEM....5**
- **B. A BASIC FORMAL MODEL FOR UNDERSTANDING CONFLICT....8**
- **C. MODES OF INTERACTION....11**
  - **1. Diplomacy....11**
  - **2. Force....12**
    - ***a. Threat of Force....12***
    - ***b. Use of Force....13***
- **D. TOOLS OF INTERACTION....14**
  - **1. Conventional....15**
  - **2. Nuclear....17**
  - **3. RMA....18**
  - **4. Cyber....19**

III. CASE STUDIES....23
- **A. OVERVIEW AND METHODOLOGY....23**
- **B. CASE STUDY 1: ESTONIA....30**
  - **1. Overview....30**
  - **2. Proposed Causal Factors....33**
    - ***a. Sophistication....33***
    - ***b. State Dependency....34***
    - ***c. Government Involvement....36***
  - **3. Value of Dependent Variable....37**
  - **4. Conclusion....38**
- **C. CASE STUDY 2: GEORGIA....40**
  - **1. Overview....40**
  - **2. Proposed Causal Factors....43**
    - ***a. Sophistication....43***
    - ***b. State Dependency....44***
    - ***c. Government Involvement....47***
  - **3. Level of Dependent Variable....49**
  - **4. Conclusions....50**
- **D. CASE STUDY CONCLUSIONS....52**

IV. CONCLUSION....57
- **A. CYBER-WEAPON ATTRIBUTES....57**
- **B. POLICY CHALLENGES AND RECOMMENDATIONS....60**

C. RECOMMENDATIONS FOR FURTHER RESEARCH 65
LIST OF REFERENCES.....67
INITIAL DISTRIBUTION LIST 71

LIST OF FIGURES

Figure 1. The Bargaining Range 8
Figure 2. Categorization of Offensive Cyber-attacks....26
Figure 3. Effectiveness of Cyber-attacks Against Estonia....37
Figure 4. Effectiveness of Cyber-attacks Against Georgia....49

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFCEA	Armed Forces Communications and Electronics Association
AFRINIC	African Network Information Center
BBC	British Broadcasting Corporation
CERT	Computer Emergency Response Team
CNN	Cable News Network
DDOS	Distributed Denial of Service
DOS	Denial of Service
EU	European Union
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
Mbps	Megabytes per second
NATO	North Atlantic Treaty Organization
PGM	Precision Guided Munitions
RBN	Russian Business Network
RMA	Revolution in Military Affairs
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
U.S.-CCU	United States Cyber Consequences Unit
USSR	Union of Soviet Socialist Republics

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife, Jennifer, and daughter, Riley, for their love, patience, and support. I would also like to thank all of the teachers in my academic career that challenged me and taught me the importance of education, particularly the importance of writing well. Lastly, I owe a debt of gratitude to Dr. Leo Blanken and CDR Jim Robinette for their advice, support, and mentoring throughout this research and writing process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

The level of dependence upon technology by state and non-state actors varies widely but is undisputedly increasing. Many states depend upon technology to help simplify and expedite complex processes such as irrigation, telecommunications, air traffic control, economic market interaction, national security, and weapons production. Counties such as the Netherlands, Canada, and Denmark have over 90 Internet users per 100 people. Less dependent counties have minimal reliance upon digital connectivity and it has little effect on the daily lives of its citizens. Somalia and Afghanistan, for example, have less than five Internet users per 100 people.[1] While the percentage of Internet users is not a direct indication of how dependent a state is upon digital connectivity, it does provide valuable insight into their degree of vulnerability. This vulnerability provides an attack surface that adversaries can exploit in order to affect the actions of a state.

An accurate grasp of the nature of a state's dependence upon networked, and vulnerable, technology is important but is insufficient to effectively affect that state's behavior. It is also essential to understand the nature and rules of state interaction. Using a common framework developed upon the structural Realist school of thought from the theoretical study of international relations, it is possible to look at how various forms of technology, and the weapons that were made available as a result of such technology, altered the way that states commonly interacted.[2] For instance, the conventional military force of a given state provides credibility based upon its capacity to inflict harm. States that have a weak military have a correspondingly low ability to affect the behavior of another state because they lack the ability to force that state's behavior. Likewise, a strong military capability normally indicates the capacity to change a state's behavior. Deterrence is the manipulation of this capability to prevent certain behavior. The horrible effects of nuclear weapons had a tremendous influence on the possessing state's ability to

[1] The World Bank, Internet Users (per 100), http://data.worldbank.org/indicator/IT.NET.USER.P2,

[2] Kenneth Waltz, *Theory of International Politics* (Random House: New York, 1979), 113.

deter another's behavior, and this relationship was further changed when opposing states both possessed nuclear capability. Significant advances in technology over the last three decades have made both conventional and nuclear weapons so precise that they altered the nature of deterrent threats. Whereas the destruction assured by the employment of nuclear weapons was a substantial aspect of its deterrent effect, recent advances in PGM and drone technology facilitated pinpoint destruction. Some of the additional benefits of this technology that affected its capacity to deter included the ability for covert employment and limited collateral damage.

The rapid increase in the capabilities of cyber-technologies has made it a nearly indispensable aspect of the developed world. Additionally, this technology has created a considerable vulnerability for its employers. Stuxnet provided the world with an example of how cyber-weapons could be used as a destructive weapon with strategic consequences.[3] The degree to which cyber-weapons could potentially affect a state that relies on digital technology is left largely to the imagination. Although international law is still murky as to when cyber-attacks constitute an armed attack, it is certainly clear that instances of cyber-attack are an increasingly occurring and persistent problem.[4] With this in mind it is essential to examine the basic characteristics of cyber-weapons and the impact that they have on interstate relations.

B. PURPOSE

The purpose of this research is to gain insight as to how the offensive application of cyber-weapons might affect deterrent interaction between states. While there is a robust body of research that examines the deterrent characteristics of conventional, nuclear, and RMA-enabled weapons, the field is still relatively nascent in its examination of offensively-employed cyber-weapons. This research intends to establish a common framework by which to examine the effectiveness of tools of force (conventional, nuclear, and RMA) and apply this framework to empirical case studies where cyber-

[3] Andrew Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate," *Joint Force Quarterly* 67, no. 4 (2012): 41.

[4] Scott Shackelford, "Estonia Three Years Later," *Journal of Internet Law* 8, no. 13 (2010): 25.

weapons were employed offensively. By examining selected and seemingly relevant factors that influence the effectiveness of a cyber-attack, the intent is to explore these causal factors specifically throughout each case study in order to draw some conclusions.[5] The conclusions should help solidify the relationship between the selected factors and consequent level of effectiveness, and thereby further the understanding of how cyber-weapons are employed to affect interaction between states.

C. RELEVANCE

This research is relevant because the continuing advances and expanding dependency upon technology create a legitimate vulnerability for an aggressor to exploit. It is imperative to understand the characteristics of successfully employed cyber-weapons and examine the factors that played a role in their ultimate level of effectiveness. This allows relevant stake-holders of cyber-policy to understand the potential dynamics that are in play when cyber-weapons are being used. In turn, it lends some predictability to assessment efforts in situations where an aggressor state may employ cyber-weapons.

Potential recommendations based on this research could advocate that possession of offensive cyber-attack capability is a useful tool with which to influence the behavior of other states. It could also reveal that the costs are too great at this time, that technology is too immature, or that there are a number of other factors which would limit or prohibit its inclusion. Examining this problem could highlight some of the policy gaps that currently exist in the burgeoning field of cyber-strategy, as well as increase the effectiveness of the nation's offensive cyber-strategy.

D. THESIS ORGANIZATION

This thesis begins by examining the underlying principles and assumptions that explain how states interact in accordance with traditional structural realist theory. One of the primary assumptions is that the international arena is an anarchic system

[5] This approach to the study of deterrence cases is outlined in Robert Jervis, "Introduction: Approach and Assumptions," in *Psychology and Deterrence*, eds. Robert Jervis, Ned Lebow, and Janice Stein (Baltimore: Johns Hopkins Press, 1985), 34.

characterized by struggle between states. A state's self-seeking behavior is tempered by the understanding that an overly aggressive approach will likely invoke response from other states.6 To refine this approach, a basic game theoretic model is presented that, given certain assumptions, demonstrates that there is always a bargaining range that is mutually advantageous to war.7 Using this as a key framework for the remainder of the research, the thesis uses a common set of criteria to characterize the effectiveness of conventional, nuclear, and RMA-enhanced tools of interaction in affecting the bargaining process. Cyber-weapons are briefly examined using this framework before applying it in depth through the case studies. The case studies examine the offensive cyber-attacks against Estonia in 2007 and Georgia in 2008 in order to determine the role that selected factors had in influencing the attack's level of effectiveness. Following the case studies, the thesis concludes with an exploratory examination of the increasing Chinese-sponsored cyber-attacks and then concluding remarks and policy recommendations that were induced from the case studies. The conclusion will also include further recommended research. Of particular note, my research indicates that state involvement generally has a limiting effect on a cyber-attack's level of effectiveness due to the desire to retain plausible deniability. As the effectiveness of an attack increases, so too does the risk of attribution. This tradeoff between effectiveness and plausible deniability is an important relationship to note. Additionally, my research indicates that the use of cyber-weapons as a tool of diplomacy does not yet have the more predictable deterrent effects of conventional, nuclear, and RMA-weapons. As a result it is suggested that the state focus on enhancing security against becoming a victim of cyber-attacks.

6 Waltz, *Theory of International Politics*, 113.

7 James Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 387.

II. FRAMEWORK

A. BASIC ASSUMPTIONS OF INTERNATIONAL RELATIONS SYSTEM

Providing structure and explanation to interaction between states is a complex process that evokes expansive theoretical arguments. Occasionally, there is such a significant external change that the body of theoretical work is drastically affected. Strategic bombing, nuclear weapons, and the technological Revolution in Military Affairs (RMA) are examples of changes in warfare capability that changed the coercive dynamics between adversaries. Many argued that theories that satisfactorily explained how states interact when armed with only conventional militaries became obsolete when nuclear weapons were developed and acquired. The dawn of the cyber-age has seen exponential increases in computing speed and capability that can be harnessed into cyber-weapons of unrealized destructiveness. In order to determine if this new technology will similarly change the system, this section examines the potential effect of cyber-weapons on classic deterrence. Subsequent case studies where cyber-weapons were used with varying success will help to identify factors that may alter the effectiveness of these weapons.

Classic deterrence theory provides a framework to explain and understand how entities interact in order to provide insight into behavior, as well as a method by which to predict behavior. The international community contains states that operate in anarchy. It is anarchic because there is not the presence of a single hegemonic power or world government that has the power to dictate the behavior of all states.[8] Because there is no such higher authority, anarchy encourages states to help themselves, thru self-help, in pursuit of ensuring their survival.[9] The patterns of interaction that result from this structure are important to examine in order to understand behavior. Fear of either unequally distributed gains or increased dependence on another state for survival are two factors that normally limit interstate cooperation because they both create an imbalance

[8] Fearon, *International Organization*, 401.

[9] Waltz, *Theory of International Politics,* 111.

of power that weaker states fear will be further exploited. This encourages states to be self-reliant and behave in a way that protects anticipated encroachment on their survival. Dependence increases vulnerability and so vulnerability is countered by either limiting dependence or strengthening the ability to control the dependent relationships.[10]

The resultant structure of the international environment is one where states act in a manner that may run contrary to the long-term stability of the system. In describing this behavior and the underlying cause Waltz provides the example of a commodity shortage. During an impending commodity shortage it is best for the greater good of the system if all consumers limit their purchase and consumption in order to ensure that everybody gets an adequate share.[11] However, the fear for survival causes consumers to purchase in bulk and hoard the commodity despite the fact that it is to the detriment of the whole. Anarchic structure of interstate relations causes much the same scenario. States act in a manner that pursues their survival even if it is not in the best interests of the system. The nuclear arms race of the Cold War is an example of this behavior. Although nuclear war was not in any state's best interests, both the United States and Russia acquired weapons in order to maintain a balance of power and ensure their survival.

The characteristics of competition set forth by Waltz and the neo-realist theorists are most useful in establishing the assumptions of state interaction because they provide a relatively simple explanation that can easily accommodate the insertion and evaluation of cyber-weapons as a tool. This theory states that relationships between interstate entities are characterized by struggle and limited accommodation under mutual suspicion. Self-seeking behavior to ensure survival is tempered by the realization that its pursuit provides a significant threat to another state. In order to prevent the other state from taking action to counter that behavior, states often accommodate and settle in order to reduce the level of tension. This decentralized behavior is constantly ebbing and flowing and causes a high degree of homogeneity among the states.[12]

---

[10] Ibid.

[11] Ibid., 107.

[12] Ibid., 113.

In order to seek the accomplishment of their goals, states can either alter their internal or external balances. Shifting internal balance means altering forces such as economic or military strength in order to affect the state's power, while external balancing indicates involvement in alliances as a way to affect the state's power.[13] Tools of interaction will be discussed in more detail later, but states in an anarchic framework use force to seek protection and advantage. The capability to use force serves as an underlying threat in all dealings with other states and generally limits extreme behavior. Without a higher government authority to which to appeal, states act in a manner that limits the threat to their survival.[14] The use or anticipated use of force by a state is likely to be met with force in response either unilaterally or in conjunction with other states. Dissection of cyber-weapon use in several case studies will help determine its effect as a tool of force in classic deterrence and provide details on the trends of its usage.

It is important to note the basic assumptions of neo-realism so that there is a commonly understood framework for understanding how and why states act. First, neo-realism assumes that the world is anarchic in that there is not a central authority that controls state behavior, but does not imply that their resultant behavior is chaotic. Secondly, it is assumed that all states possess some degree of offensive military capability that can be used to inflict pain on another state. Because a state can never positively be sure of another state's intentions, it is necessary to factor the offensive military capability into decision-making as states must always assume that another state may resort to use of this capacity to affect behavior. That survival is the driving force for state behavior is the fourth assumption of neo-realism, while the fifth is that states develop a strategy that best ensures their survival. This rational development sometimes leads to miscalculations because all relevant information is not always known.[15]

---

[13] Ibid, 116–128.

[14] Ibid.

[15] John Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (1994): 10.

B. A BASIC FORMAL MODEL FOR UNDERSTANDING CONFLICT

Having defined the basic structure and characteristics of interstate anarchy allows for a more detailed examination of how states interact and under what conditions they would come into conflict. Using the Waltz as a baseline theory on anarchic interaction, Fearon examines traditional realist theory and argues that based on its assumptions its conclusions do not logically follow. Specifically, the expectation that benefits will be greater than costs, rational preventive war, and rational miscalculation due to either lack of information or a disagreement about relative power are not sufficient causes to explain why states come into conflict. With war being a costly and risky endeavor, Fearon uses a basic game theoretic model to demonstrate that there is always a bargaining range that is mutually advantageous to war.[16]

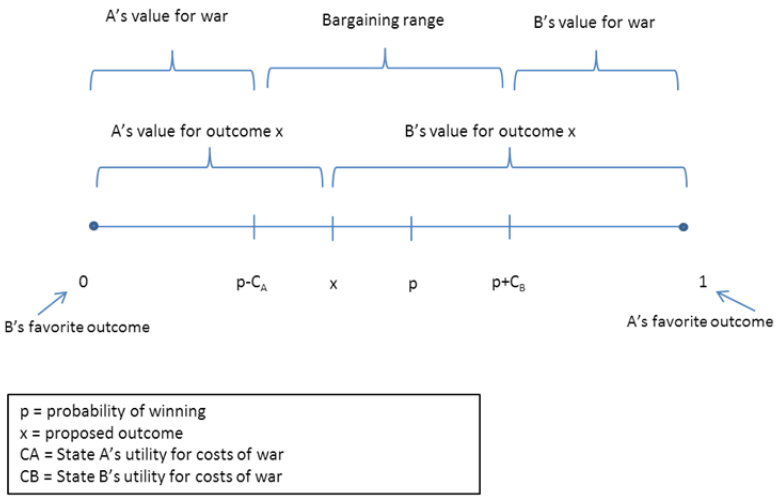

Figure 1. The Bargaining Range[17]

The bargaining range (Figure 1) is a linear range with each actor's desired end-state at opposing ends of the line. Between those two opposing points takes place a "dance" with each side essentially sizing the other up to determine their opponent's capabilities (probability of winning) and resolve (utility of costs).[18] With perfect and

16 This assumes risk-neutral or risk-averse actors.

17 Fearon, *International Organization*, 387.

18 Ibid.

complete information the bargaining range is also clear which makes war more costly than a bargain. To demonstrate this theory using a candy bar: if two states go to war over a candy bar, and the cost of the war is 20 cents, then after the war the value of the candy bar is 80 cents. Because the candy bar is of less value, the subsequent division of the candy bar will also be of less value. Had the states decided to bargain rather than fight, then they could have divided up the full candy bar. [19] Using the probability of winning (p) and the utility of the costs for war (C_A or C_B), Fearon demonstrates how states can settle upon a bargaining range. [20] Understanding this logic, Fearon argues it is a puzzle why states would ever fight. [21]

He posits that there are three answers to this puzzle of why states come into conflict. First, states may have private information and the incentive to misrepresent it during the bargaining process.[22] The second reason is that under certain conditions a state cannot successfully commit to a bargained outcome, while the third reason deals with the indivisibility of goods and consequent difficulty in bargaining.[23] Fearon contends that commitment problems and issue indivisibility are of secondary importance and that private information and the desire to misrepresent it is more commonly the reason that states come into conflict. It is important to understand the mechanics of this argument before examining cyber-weapon case studies in order to better understand the decision-maker's potential goals and objectives in using such a tool.

States inherently possess private information about their capabilities and resolve. Because war is more costly than a mutually-beneficial bargain, states benefit from communicating about intentions and capabilities in order to prevent miscommunication and subsequent miscalculation. There are, however, situations in which states purposely withhold or misrepresent private information. Although states want to avoid costly war,

---

[19] Leo Blanken, slideshow *Fearon and the Puzzle of Conflict: Unitary Rational Actors Choosing War*, obtained from https://cle.nps.edu/xsl-portal/site/3b74a4a9–2968–4d06–8c54-cc0643ec9c61/page/1025a83a-f0ee-4015–8938–16d32223dbb1.

[20] E(u) = (100*.5) + (0*.5)—20 = 30

[21] Fearon, *International Organization*, 383.

[22] Ibid., 391.

[23] Ibid., 401.

they also want to get a good deal out of bargaining. This can lead to intentional exaggeration of one's technological capability or willingness to fight in order to affect the adversary's decision calculus regarding his probability or cost associated with winning. If a state can falsely and successfully bolster their probability of winning in their opponent's eyes, then they have affected the bargaining range to their benefit. Their adversary, thinking his probability of winning is now reduced is likely to accept a less advantageous bargain than had information been accurately represented. Similarly, a state may wish to misrepresent private information regarding their true resolve towards an issue or a known weakness in order to protect a more beneficial bargaining range.[24] States often revert to costly signaling to augment the believability of their misrepresentation with a force-related maneuver such as weapons production, troop mobilization, support to foreign troops, or engagement in alliances or treaties.[25] States implementing this strategy must be aware that their actions could induce the enemy to reject the new bargaining range and opt for war, as intentional misrepresentation often increases the possibility of miscalculation. This possibility may affect the state's ability to implement this strategy as it is necessary to base the costly statements on what a state is realistically willing to do.

It is important to note that private information and the incentive to misrepresent it come into play in two other rationalist scenarios for conflict. Conflict may be used to prevent potential or actual adversaries from making inferences about a state's private information. For example, American intervention in Vietnam was arguably intended to signal to the USSR that the United States placed great value on stopping the spread of Communism. Failure to intervene would likely have indicated to the USSR that they could freely expand their aggression without American exception.[26] This tactic is also commonly employed by weak states that want to create the perception that they are stronger or harder to subjugate than may actually be the case. By engaging in conflict and appearing as a costly adversary, the state hopes to increase its bargaining ability in future

[24] Ibid., 396.

[25] Ibid.

[26] Ibid., 400.

negotiations.[27] Conflict can also offer an opportunity for a state to demonstrate private information about its military capability with the intent to create an impression in the minds of adversaries. States of increasing power may force conflict in order to demonstrate their power on the world stage. Similarly states in perceived decline may view conflict as a means of demonstrating their resiliency and continued strength.[28]

C. MODES OF INTERACTION

The tools of interaction highlight the typical escalation process of a conflict from peace to war. Ideally, states interact to find solutions through diplomacy. Should diplomacy fail, then the interaction escalates to one in which force is threatened to influence an adversary to behave as dictated. The actual use of force is the final stage in this interaction if the threat of force does not alter the adversary's behavior. It is important to highlight some of the characteristics of each stage before examining the case studies in order to understand how cyber-weapons as a tool of deterrence affect the "dance" in the normal escalatory stages of a conflict.

1. Diplomacy

With a baseline understanding of the characteristics of an anarchic international relations environment, how states interact, and the conditions under which states come into conflict, it is possible to examine the tools that states commonly use in their interaction. Diplomacy is the method by which states can interact and settle differences without resorting to war. Each actor pursues its goals while always maintaining state survival as the primary objective. When goals conflict, states exchange demands and through a process of bargaining and communicating the states agree on a solution that is mutually advantageous when compared to post-conflict possibilities. Underlying all interaction and bargaining is the implication that force may be used by either actor in order to achieve their objectives. A mutual understanding of the adversary's relative power helps to define the risks and costs of war and thereby establish a bargaining range

[27] Ibid.

[28] Ibid.

within which the states seek a solution.[29] Solutions within the bargaining range are not ideal for either party, but they pose less risk than the alternative of going to war.[30] Although Fearon's model demonstrated that settling on a bargain is less costly to both sides than going to war, the underlying implication of force makes it necessary to develop and prepare these tools of force should they become necessary.

2. Force

It is important to highlight that tools of force are essential in both the bargaining and conflict phase of state interaction. Their importance in conflict is obvious, but in the bargaining phase the capacity of the force directly affects the probability that a given state will prevail. The following discussion examines force as a threat and as a physical impetus to cause change.

a. Threat of Force

Deterrence and coercion are the two primary means by which the threat of force is employed. State A seeks behavior from State B and threatens to use force to ensure the achievement of that behavior. In deterrence, the threat of force seeks to prevent a change to the status quo, whereas coercion uses threats to force a particular behavior. Several variables feed this interaction which is best understood using Fearon's model of probabilistic rational behavior between anarchic states.

The capabilities of State A's threat affect the probability that State A will prevail. In an environment where adversaries understand the other's intentions and power, the threat of force results in a set bargaining range within which negotiations take place. In determining the effectiveness of certain weapons in a deterrence framework, it is important to understand their effect on the probability of prevailing in conflict. Deterrence relies on a combination of the threat's capacity and the state's resolve to establish a bargaining range that prevents alteration to the status quo.[31] This concept will

---

[29] Ibid.

[30] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 1.

[31] Robert Art, "To What Ends Military Power?," *International Security* 4, no. 4 (1980): 6.

be examined in detail in subsequent sections. On the other hand, coercion explores how threats force an adversary to take action. In providing weight to the threat of force theory, Shelling explored the concept of diplomacy of violence in his book *Arms and Influence* and explained the coercive elements of violence. His research shed light on how violence could be threatened in order to force an opponent to perform a desired behavior regardless of intent or what level of violence was applied.[32]

George furthered the concept in *The Limits of Coercive Diplomacy* in which he explained the tenets of coercive diplomacy theory and distinguished it from the more offensive use of coercion, or compellence, as advocated by Schelling. According to George's model, coercive diplomacy was a strategy that sought to preserve the status quo by either halting an ongoing action or reversing action already taken. The theory provides flexibility in that it allows policy-makers to select the urgency, punishment, and incentives based upon the factors of a given scenario.[33] It is important to note that George's theory was not limited to military force, but also allowed for diplomatic, economic, psychological, and other forms of punishment.[34] Additionally, this strategy has varying levels of enforcement so that the coercing state can best manage influence over their adversary. The leveraged punishment in this theory, whether threatened or actually employed, was exemplary in that it did not strive to bludgeon an opponent into submission, but rather serve as an impetus to make changes.[35] Ideally, the adversary responds positively to the threats to which they have been subjected so that escalation is not necessary.

b. Use of Force

Outside its use as a threat, force can be either offensive or defensive. Defensively, force can respond to and affect the damage imposed by an adversary's use of force. Specifically force can repel an attack or serve as a first-strike capability in

---

[32] Schelling, *Arms and Influence*, 3.

[33] Alexander George, *The Limits of Coercive Diplomacy* (Boulder, CO: Westview Press, 1994), 16.

[34] Ibid., 29.

[35] Ibid., 10.

response to an anticipated attack.[36] Should the threat of punishment fail, states in an anarchic environment may resort to the offensive use of force to settle their differences. As previously discussed, because rational actors understand that conflict is inherently more costly than settling on a bargain, this scenario is the result of very limited rational factors. The use of force indicates a failure of doctrinal deterrence, but coercive diplomacy allows the use of force as part of the interaction between states. In this scenario force is incrementally and sparingly employed as an indication of two things: that the adversary has the opportunity to revert to the status quo, and that failure to do so will incur the application of more force.[37] Offensive force can also compel an adversary to take a desired course of action away from the status quo, but this research focuses on the rational application of force to preserve or reestablish the status quo.

D. TOOLS OF INTERACTION

Deterrence theory has long attempted to explain how states use threats to prevent an adversarial state from taking specific undesired behavior. The deterring state must have the power and capability to exert the required influence, the threat expressed must be credible, and this threat must be communicated to the adversary.[38] In terms of Fearon's model, it seeks to alter the cost equation in a way that makes the cost of conflict unacceptable to an adversary. The adversary's decision calculus to stop the menacing behavior is affected by how they perceive the credibility of the force, the deterrer's willingness to employ it, and how effectively the effects can be avoided.[39] If the adversary associates little cost to the threat, or can easily mitigate the costs, then the deterrent has little effect and the strategy is likely to fail. The concept and theory of deterrence is historically woven throughout conflicts, but the theory attracted real attention and refinement with the introduction of nuclear weapons and the ability to

---

[36] Art, *International Security*, 6.

[37] George, *The Limits of Coercive Diplomacy*, 2.

[38] T.V. Paul, Patrick Morgan, and James Wirtz, eds., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, Chicago, 2009), 2.

[39] Ibid., 309.

inflict tremendous death and destruction upon an adversary. Although it plays a prominent role, it is important to highlight that deterrence theory contains more than nuclear deterrence.

In order to measure the effectiveness of different tools of deterrence, it is necessary to examine them using a common set of criteria. By applying a similar framework it is possible to reduce complex methods of deterrence into a set of attributes by which they can easily be compared and contrasted. This section briefly examines conventional, nuclear, Revolution in Military Affairs, and cyber-deterrence in terms of the following questions:

- What is the potential level of destructiveness?
- Are the effects controllable?
- What level of control does the state have in initiating the use of the weapon?
- Does use of the weapon allow for plausible deniability?
- Can the weapon be used covertly?
- Is the weapon operational or strategic? (i.e.—can it directly hit a target or does it have to fight through the enemy?)
- Is it contestable?
- Is it likely to evoke an asymmetric response?
- Is it costly to develop or use?

This initial examination of the deterrent attributes of cyber-weapons is far from conclusive. Application of the attribute framework to several case studies allows for the induction of initial conclusions regarding how cyber-weapons affect the classic deterrence "dance" between actors in a conflict.

1. Conventional

Conventional deterrence is the management of traditional tools of force such as ground forces, air forces, and navies to prevent or reverse an undesirable behavior. The gamut of conventional means runs from minimal application of force to high-intensity full scale combat depending upon the capability and level of threat that the deterring state wishes to convey. The potential level of destructiveness spans from minimal,

demonstrated by one soldier firing his weapon in response to an adversary's provocative behavior, to extraordinary, demonstrated by the Allied forces invasion of Europe in 1944. Deterrence through means of conventional weapons has great potential for collateral damage, but the amount of collateral damage is generally proportional to the intended level of destructiveness. For example, one infantry company is likely to cause less collateral damage than a carpet bombing operation.

The state is able to exercise strict and exacting control over conventional means of deterrence because these tools are normally arms of the state's power establishment. For the scope of this examination, tools of conventional deterrence are assumed to be under state control. This relationship consequently makes plausible deniability by the state almost impossible. In terms of the ability to covertly employ this means of deterrence, conventional deterrence is second only in difficulty to nuclear deterrence. Although small-scale conventional deterrence can be executed covertly, smaller conventional tools are also less effective in their ability to deter. Large and significant demonstrations of conventional weapons are necessary in order to have a deterrent effect, but this also decreases the ability to covertly employ them. With respect to the level of employment, conventional deterrence weapons can be either operational or strategic. The strategic bombing campaigns of World War II provide examples of how the capabilities of conventional forces could be used directly against strategic centers of gravity, while the large-scale ground invasion forces of Desert Storm highlight deterrent capability at an operational level. The use of conventional deterrence is highly contestable in the sense that an adversary state may believe it possesses an effective counter or defense to the deterrent threat.[40] This gray area can complicate the efforts of the deterring state. Finally, with respect to cost, conventional means of deterrence are expensive due to the quantity of troops and equipment necessary to increase effectiveness, as well as the number of casualties that a state must be willing to accept. This is largely due to the fact that greater deterrence comes from a more significant threat which equates to a large number of forces and weapons. Additionally, in order to reduce the contestability of conventional deterrence, states must seek to demonstrate an overwhelming advantage. Significant

[40] Paul et al., *Complex Deterrence*, 309.

buildup and preparation are normally essential in order to convince the adversary that their behavior is creating a legitimate threat response.[41]

2. Nuclear

The physical and psychological destructive power contained by nuclear weapons was unparalleled by any weapon in history, and as such it had a profound effect on deterrence doctrine. Although modifications can be made to the size of the nuclear weapon, the destructive capability remains intense. The destructiveness introduced a weakness because the stigma of nuclear weapons was so powerful that it had limited effectiveness to control anything short of total war. While it was effective in preventing total war during the Cold War, nuclear-armed states took smaller actions that could not rationally or proportionally exact a nuclear response. Additionally, the effects of nuclear weapons were controllable only to the degree that a state could select the target area. Once detonated anything within a given radius was equally subjected to the destructive powers of this weapon.

Although the break-up of the Soviet Union and subsequent expansion of the nuclear black market made nuclear weapons available to non-state actors, the preponderance of nuclear material remains under state control.[42] The ability to use nuclear weapons within these states typically resides in a very small group of people and the state thereby has significant control over tools of nuclear deterrence. With the exception of relatively small amounts of nuclear material that may have fallen into the hands of non-state actors, state control makes plausible deniability very difficult.[43] Furthermore, the telltale signs of nuclear detonation make covert use of this weapon nearly impossible. Although nuclear weapons can be used tactically, the greater deterrent effect is gained by large-scale threats directly against strategic centers of gravity such as population centers.

---

[41] Fearon, International Organization, 401.

[42] Federation of American Scientists, "Status of World Nuclear Forces," December 2, 2012, http://www.fas.org/programs/ssp/nukes/nuclearweapons/nukestatus.html.

[43] Council on Foreign Relations, "Loose Nukes," December 2, 2012, http://www.cfr.org/weapons-of-terrorism/loose-nukes/p9549.

Perhaps the most significant aspect of nuclear deterrence theory was that the effect of nuclear weapons was uncontestable. This attribute is the foundation of nuclear deterrence and once the USSR and the United States secured second-strike capability it had a mutually deterrent effect that resulted in four decades of peace. Although those four decades were the equivalent of a hostile chess match, there was nevertheless peace. The threat of asymmetric response was not historically a concern of nuclear deterrence because a nuclear strike was considered to be the worst type of attack. A far greater concern was the level of nuclear retaliation. In terms of cost, the greatest cost of nuclear weapon deterrence arguably comes from strong public opposition to their use. The first, second, and third order effects of this weapon make the cost of its use in a first-strike scenario almost prohibitive.

3. RMA

The RMA is the use of rapidly changing technology to enhance war-fighting means and methods. The specific and accurate employment of force increases the flexibility of deterrence by allowing for a range of policies and techniques that can be used against an adversary. Nuclear deterrence during the Cold War prevented large scale nuclear war, but was ineffective against lesser conflict. The precision of RMA enables it to efficiently cover the gaps that conventional and nuclear deterrence could not. By enhancing the capabilities of the tools of nuclear and conventional deterrence, RMA altered existing cost equations and thereby had a profound effect on deterrence. Just as conventional deterrence spans the gamut of destructibility based upon desired effects, so too does RMA-enhanced deterrence. The precision of these weapons allows both the destructiveness and the effects to be closely controlled with collateral damage minimized.

State control is not vastly different from conventional and nuclear weapons because RMA is applied to those same weapons. Similarly, the ability to plausibly deny or covertly employ these weapons is not greatly affected with RMA advances. With the exception of small-scale covert operations such as assassinations, RMA-enhanced deterrence still relies on the capacity to inflict destruction to be effective. Destruction caused by weapons that are traditionally state-controlled is difficult to deny or hide.

RMA increased the strategic capability of conventional means of deterrence by making it possible and relatively easy to execute pinpoint destruction from great standoff ranges. In affecting the decision-making cycle of an adversary state it is possible to target specific capabilities or even decision-makers, rather than engage in massive conventional battles that attrite the enemy's military force in order to affect its decision-making apparatus. While the RMA also increased the precision of nuclear weapons, it did nothing to reduce the associated costs of using these weapons and therefore had little effect on its strategic value.[44] As contestability was an issue with conventional rather than nuclear deterrence, it remains an issue with RMA deterrence.[45] The deterring state must execute the dance in such a manner as to convince the adversary that its technological advantage is beyond contestability. In terms of evoking an asymmetric response, the RMA did not greatly alter the threat of either conventional or nuclear deterrence to cause this. Because the effects are so precise, the deterring entity faces a lower cost threshold for involvement due to the limited collateral damage of a precisely employed RMA force.[46] The RMA not only reduces adverse public reaction but provides decision-makers with a flexible range of options by which they can effectively increase their resolve on an issue without risking the commitment of large forces or mutually assured destruction. Increased and believable resolve bolsters the deterring state's credibility.[47] While these are marked advantages of the RMA, this ease of use can also foster overreliance on these weapons or even affect the cost equation in a manner that could increase the likelihood of war.

4. Cyber

The RMA touches on some of the technological advantages that cyber-weapons produce, namely the precision targeting ability, but the field needs a more thorough examination in order to determine the specific impacts, advantages, disadvantages, and considerations that this burgeoning tool has on deterrence. The potential level of destructiveness of cyber weapons has the largest variance among the types of deterrence.

---

[44] Paul et al., *Complex Deterrence,* 309.

[45] Ibid.

[46] Paul et al., *Complex Deterrence,* 309.

[47] Ibid.

Some documented instances of cyber weapon use include nothing more than offensive alteration of adversary websites, while the other end of the spectrum has the potential for great destruction. Although the most extreme actual use of cyber weapons includes physical destruction of equipment, it is possible for this weapon to be harnessed in such a way as to create the loss of life.[48] The effects of cyber weapons also vary widely. Because developments in computer science are a large part of the RMA, certain cyber weapons can be very precise in their targeting and almost eliminate collateral damage. However, many of the more commonly used cyber weapons work by spreading like a contagious illness, which obviously makes controlling the collateral damage nearly impossible. Additionally, when targeting networks or control systems it is also very difficult to predict the second and third order effects of an attack.

Two of the more compelling reasons to examine the deterrent effects of cyber weapons are that they are used by actors in addition to the state and they also provide the user with plausible deniability. In fact, a preponderance of recent acts involving cyber weapons contains significant attribution problems. When this is combined with the capacity to be surgically employed, its capacity for covert employment becomes clear. Cyber weapons can be used either operationally or strategically depending upon the desired effects, although there is a much higher threshold of expertise necessary to utilize this weapon in a strategic manner. Contestability is an interesting aspect of cyber war because the specific capabilities of weapons that an actor possesses are closely guarded secrets. As such, it is very likely that an adversary forms a potentially uneducated opinion as to the effectiveness of their defenses.[49] Because cyber weapons possess the ability to inflict significant damage and many states lack the ability to respond in kind, the potential to evoke asymmetric response is a very legitimate threat. In terms of cost, cyber weapons have similar considerations as do RMA-enhanced weapons. While there is a lower threshold for use because of the precise effects and potential for limited collateral damage, there is an increased potential for misuse. One curious aspect of the cost relates

48 Andrew Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate," *Joint Force Quarterly* 67, no. 4 (2012): 41.

49 Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: The RAND Corporation, 2009), 79.

to public opinion as cyber weapons seem to evoke less adverse public opinion that may be surmised. This could perhaps be due to the problems of attribution. Some additional issues that need further development include the effectiveness of this weapon across the spectrum of conflict, how to measure the effectiveness its use, and a myriad of legal concerns.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES

A. OVERVIEW AND METHODOLOGY

The objective of these case studies is to examine the effectiveness of offensively-used cyber-weapons in order to form some propositions regarding their potential contribution to classic conception of deterrence.[50] Significant research exists about conventional, nuclear, RMA, and defensive cyber deterrence, but the resources are less abundant in looking at how offensively-employed cyber-weapons affect the diplomatic, including coercive, interaction between states in a conflictual relationship. The case studies developed in this research will not provide finality to this question, but rather intend to induce some conclusions that will further the body of research. It is important to research this because the use of cyber weapons is becoming more prevalent and has the capability to inflict tremendous damage. When potentially revolutionary tools of diplomacy, such as nuclear weapons, were introduced in the past it was critical to evaluate exactly how they would affect the relationship between actors, and so it is important to now examine how offensively-employed cyber weapons might affect interstate dynamics.[51] Additionally, insight gained will help to develop policies to harness and exploit the power of offensive cyber weapons, as well as defend against their use by adversaries.

The case study methodology used will be inductive in that lessons will be drawn from empirical examples after looking at the relationship between potential causal factors and the resulting depth and breadth of the attack.[52] Two conflicts have been selected where cyber weapons were employed as an offensive tool of diplomacy with the intent of subversion of a state's ability to govern.[53] Because this weapon allows for a wide variety of effects, cases were selected where the intent of the aggressor states were similar. This

---

[50] Bernard Brodie, *Strategy in the Missile Age* (Santa Monica, CA: The RAND Corporation, 1959), 271.

[51] Fred Kaplan, *The Wizards of Armageddon* (New York: Simon & Schuster, 1983), 33.

[52] Alexander George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (MIT Press: Cambridge, MA: 2005), 21.

[53] Thomas Rid, Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 22.

is meant to help isolate and attribute the role that the proposed drivers of effectiveness actually had on the attack's level of impact. As an example, although both are cyber-attacks, commercial website defacement and digital destruction of a nuclear reactor control system have vastly different intents which make it difficult to determine the role of causal factors.

The case studies seek to determine how a host of proposed causal factors might influence the effectiveness of offensive cyber-attacks executed under similar intent.[54] Effectiveness of the attack is the dependent variable of this study and is defined as the level of impact the attack had on disrupting the society and undermining the government's ability to continue successful governance. The measure of effectiveness will be described by evaluating the breadth and depth of each attack. The breadth of the attack describes the proportion of the target group that was attacked. For example, if an attack aimed to cause denial of service for the entire governmental digital infrastructure, but only affected a small portion of the judicial system, then the breadth of the attack is very minimal. Meanwhile, depth assesses the severity of the attack on the successfully targeted group. For instance, even though only a small portion of the judicial system was successfully targeted in the previous example, the effect of that attack will determine the depth. If the judicial system's connectivity was unavailable for thirty minutes, then the depth of that attack is shallow, whereas if the judicial system saw all of its data and records destroyed beyond repair, in addition to physical damage to the IT infrastructure, then that obviously demonstrates a much deeper attack.

It is important to mention that it can be difficult to neatly categorize offensive cyber-attacks because there are many unknown variables that determine the breadth and depth of the attack. Much of the data regarding empirical examples remains highly guarded because its release could incriminate responsible parties or provide critical access to weapons development and implementation to an adversary. Some attacks may have a narrow breadth and shallow depth due to the relative inexperience of the aggressing force, while it could also be attributed to the aggressor's desire to retain

[54] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 69.

plausible deniability or merely serve as a nuisance to the targeted state. Wide breadth and shallow depth could also be attack characteristics of a state with these same intentions, or of a large but uncoordinated botnet army.[55] On the other hand, a narrow but deep attack could be executed by a government looking to cripple a specific target, or a small but coordinated effort on the part of a group of hackers. Attacks that are both wide and deep require not only significant assets in terms of either numbers or technologic sophistication, but also a large coordination effort. The state is arguably the only entity that could muster this level of effort, but to do so could jeopardize their ability to remain anonymous. There is not any empirical evidence of an attack that maximized the breadth and depth of their effects. So, while unknown factors may complicate attempts to understand precisely why a cyber-attack had a particular combination of depth and breadth, the case studies selected seek to highlight some trends between the proposed causal factors and the resultant level of impact.

Figure 2 is a tool that describes the combined characteristics of offensive cyber-attacks along the ranges of depth and breadth. This tool is important because it helps establish a common framework that that can be used with different case studies to help understand the range of an attack's level of impact.[56]

---

55 Martin Libicki, *Cyberdeterrence and Cyberwar*, 17.

56 Gary Goertz, *Social Science Concepts: A User's Guide* (Princeton: Princeton University Press, 2006), 35.

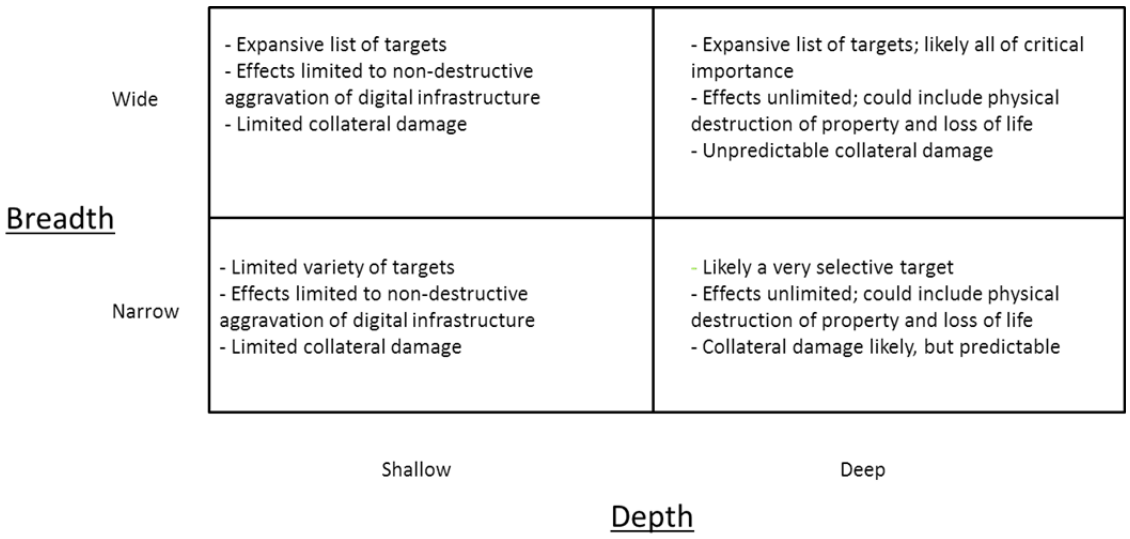

Figure 2. Categorization of Offensive Cyber-attacks

In order to highlight how these characteristics might look, the following discussion provides a hypothetical walk through a scenario in each quadrant of the above chart.[57] Potential causal factors will be excluded so that the range of the dependent variable (level of impact) is the only variance. The range of both breadth and depth is a continuum, so there is not a clear distinction when an attack crosses from one quadrant into the next.[58] The examples provided below attempt to demonstrate scenarios that are clearly within each quadrant.

Beginning in the lower-left quadrant with an offensive cyber-attack that is shallow in breadth and narrow in depth, the characteristics are a limited variety of targets that are attacked to a level that does not cause long-term, sustained, or irreversible damage. The target could be a very specific individual or capability, such as the California Supreme Court, or it could include a broader sector such as electrical power control stations in the western United States. In this example, shallow depth could indicate that the websites of the California Supreme Court are defaced with pro-Communist rhetoric or are not accessible for a couple of hours. Although important, defacement or lack of availability of Court digital services is relatively insignificant to

[57] Goertz, *Social Science Concepts: A User's Guide* , 35.

[58] Ibid., 34.

the average citizen for a couple of hours. Shallow attacks on the western United States electrical power grid could also include temporary power outages. The effects of this attack are also relatively minor, although there is an increased potential for loss of life which arguably makes this a less shallow attack than the California Supreme Court example. Although roused, citizen concern is at a low-level because of the limited scope and destruction associated with an attack in this quadrant. Because the attack is selective in its targeting and limited in the destructive capacity, the collateral damage is likely to be predictable and controlled.

The upper-left quadrant is wide in breadth but shallow in depth. The scope and variety of targets is much vaster and could include several different sectors, while the effects of the offensive cyber-attack are similar to the previous example. An example of the breadth of such an attack could include the simultaneous targeting of the digital infrastructure of the federal government, air traffic services, financial institutions, defense warning systems, and power stations. Because the attack is still narrow in depth, the effects are relatively limited in comparison with what could possibly result. This could include a temporary or intermittent denial of service. This attack has a significant impact on the average citizen because the scope of targets spans a major portion of services on which they rely. Normal daily life, for the duration of the attack, would not be possible. A state of panic would certainly ensue tempered only by the fact that the impact is narrow in depth. Government attempts to restore critical services are successful and there is limited data or physical destruction. The likelihood of collateral damage increases with the breadth of the attack because the second and third order effects of such a vast attack cannot be reasonably be predicted.

An attack in the lower-right quadrant is narrow but deep. The scope of the targets is very selective and narrow, but the damage done begins at significant and moves towards unlimited. Some examples of this are an attack on the air traffic control services that destroy the database of airborne flights, disable air to ground communication, alter data provided by navigation beacons, and turn off runway and beacon lighting. A particular bank could also be the target where the cyber-attack alters the account information, including balances, of the bank’s customers. Back-up servers, databases, and

records would also be altered or deleted so that the bank could not easily rectify the damage done by the attack. These are very selective attacks on specific targets, but the intended level of destruction is substantial with significant loss of life and permanent elimination of financial savings only examples of the potential effects. Immediate attempts to defend against the attacks or counter the effects meet with very limited success. Similar to the effects of September 11th, such a spectacular attack will spur great concern among the citizens, but will be tempered by the fact that only a small percentage of the population was targeted. While the collateral damage of narrow attacks is generally low, the depth of the attack makes some side effects unpredictable.

The upper-right quadrant shows the characteristics of the worst-case cyber-attack. This attack is both wide and deep. Attacks of this variety will be against numerous targets and seek maximum destruction or disruption. As in the example for the upper-left quadrant, the target could be the digital infrastructure of the entire federal government, air traffic services, financial institutions, defense warning systems, and electrical and nuclear power stations, but the effects are much worse. An attack of this magnitude would likely totally cripple the digital infrastructure, destroy critical data, or inject malicious data that cause systems to operate in a destructive manner. Supervisory control and data acquisition systems (SCADA) that control the functions of power, nuclear, sewer, and air defense systems (among others) could either be crippled or engineered to create massive nuclear and biological emergencies. Additionally, attacks could modify or erase accounting data at financial institutions, usurp all forms of digital communication, turn off pace-makers, render air defenses useless, and even gain control of a state's sensitive satellites. Government attempts to counter or defend against an attack of this nature would be limited and piecemeal. Pandemonium would certainly ensue as the citizens realize their government cannot protect them. Within this range it is important to remember that the intent of these attacks is not to kill people, although that may be collateral damage, but rather to cause massive disruption to the people and the government's ability to effectively govern. The target is strategic rather than tactical, although tactical disruption or destruction is highly probable. The target is the emotions

of the people, rather than a physical entity such as a uranium enrichment facility.[59] Collateral damage is most unpredictable in this quadrant and not likely to be of concern to the aggressor.

This research presents two case studies and examines three proposed causal factors in order to determine the role that they played in affecting the attack's level of impact. The case studies are the 2007 attacks against Estonia and the2008 attacks against Georgia. There are several variables from which to choose, but the three that will hopefully allow for the most refinement and valuable insight are the level of attack sophistication, role of the alleged adversary government, and dependency of the target upon cyberspace technology. While there is variance in the dependent variable, the lack of empirical examples prevented a truly broad range of variance. There are two reasons for this. First, thankfully there has not yet been a cyber-attack that has been both wide and deep. Secondly, most cyber-related data are not disclosed by governments in fear that it will provide advantage to the adversary.[60] Therefore, there are likely more cases of cyber-attack, but they are not publicly available.

Measuring the effectiveness of an attack is a difficult and contentious field that is subject to innumerable qualitative and quantitative aspects depending upon the evaluator. While there is limited quantitative data for these case studies, it relates to very specific technical effects and fails to accurately represent the aggregate effect of the attacks. It is therefore necessary to focus mainly on the qualitative data to develop an accurate picture of the level of impact each attack had. Most of this data comes from post-incident reports performed by government agencies, non-government organizations, and media. Each case study presents a brief introduction followed by an examination of the independent variables, which are the proposed drivers of effectiveness, a discussion of the cyber-attack's level of impact, and a conclusion.

---

[59] Ibid., 22.

[60] Libicki, *Cyberdeterrence and Cyberwar*, 17.

B. CASE STUDY 1: ESTONIA

1. Overview

Estonia is one of the most digitally developed nations in the world. For the past century the country has been subject to many masters as World War I, II and the Cold War ravaged Europe. When the Soviet Union fell in 1991, Estonia finally regained its independence and set a course for technological development. Many years ahead of the wireless boom, the country made an astute decision to replace landlines with wireless technology. Currently cell phone saturation is over 100 percent and the nation's citizens are heavily reliant on digital technology to vote, bank, pay for parking, and a host of other activities. In fact, 80 percent of Estonians rely on the Internet to do their banking and vote.[61] Although Estonia had gained its independence, approximately 30 percent of its population was Russian due to Russian emigration and ethnic resettling practices.[62] This population provided the Russian government with a powerful means of leverage within Estonia. Estonia moved forward and attempted to enhance their culture and security by joining NATO in 2004 and later making fluency in the Estonian language a requirement for citizenship, an obvious message to the significant ethnic Russian population.[63] On 26 April 2007, the final anti-Russian action by Estonia was the move to transfer the Bronze Soldier, a statue of a Russian soldier erected in 1947, and accompanying remains of Soviet troops felled in taking Estonia in World War II from the capital of Tallinn to a more remote area. To Estonians the statue had become a symbol of oppression, while to Russians it was a rallying point.[64] To both groups it became a very contentious site that the Estonian government decided to move. Although Estonian officials claimed it was to provide a more suitable resting place, many Russians believed it was assert their power and subjugate the ethnic Russians.[65]

---

61 Richard Stiennon, *Surviving Cyber War* (Lanham, MD: Government Institutes, 2010), 86.

62 Central Intelligence Agency, "1992 World Factbook: Estonia," December 14, 2012, http://nodedge.com/ciawfb/.

63 Stiennon, *Surviving Cyber War*, 87.

64 Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Prespective," *Proceedings of the 7th European Conference on Information Warfare*, Academic Conferences Limited (2008): 1.

65 Ibid.

The response to the statue's removal was immediate, surprising, and difficult to attribute. Beginning 27 April 2007, Estonia became victim to a massive cyber-attack that lasted 22 days. The attack targeted financial, communications, and government infrastructure sites as well as the personal communication devices of government officials.[66] The attacks were mainly distributed denial-of-service (DDOS), which essentially impair websites and lines of communication by introducing an overwhelming amount of traffic, but there were some more sophisticated SQL attacks intended to hack into selected systems.[67] Of note, two of the nation's largest banks were offline for over two hours and subsequently unavailable to anybody outside of Estonia for several days, as a mitigation effort was to shut down all interstate online access. Attacks on several government Internet service providers (ISP) servers allegedly interrupted government communications for a short amount of time. Propaganda attacks also targeted the Estonian Prime Minister's website and placed a fake letter of apology to the Russian people with a promise to relocate the Bronze Soldier.[68] There were reportedly over 80,000 different IP addresses from which the attacks were launched and most of them were outside of Estonia.[69] Specific instructions for what and how to attack were in Russian on many common Russian blog sites and also contained very apparent political motivations.[70]

In addition to the cyber-attacks, pro-Russian riots erupted on the streets of Tallinn also beginning on 27 April. While ignoring the looting and destruction, Russian media called them "peaceful protestors." Police action against the rioters agitated Russian government officials and even moved one official to state that it was a call for war.[71] Government-backed members of Nashi, a Russian political youth movement, rioted at the

---

66 Stiennon, *Surviving Cyber War*, 87.

67 Ottis, *7th European Conference on Information Warfare*, 3.

68 Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *Cooperative Cyber Defense Center of Excellence*, http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf .

69 Stiennon, *Surviving Cyber War*, 87.

70 Ottis, *7th European Conference on Information Warfare*, 3.

71 Ibid., 2.

Estonian embassy in Moscow and prevented workers from entering or departing. The Estonian ambassador to Russia was also physically attacked on two different occasions while the rioting was taking place.[72] The Russian government itself stopped certain rail and commercial truck exports to Estonia under the guise of maintenance that needed to be performed and Estonian businesses suffered loss of revenue and contracts with prior Russian partners.[73] Additionally, in early May members of the Russian Duma travelled to Tallinn to call for the resignation of the Estonian government.[74]

Although Estonia was able to reinforce their digital defenses, the cyber-attacks reached a crescendo on 9 May and then began to taper.[75] This was a day of national significance in Russia as it marked their victory over Nazi Germany in 1945. Several investigations into the attacks failed to positively attribute the responsible organizations although circumstantial evidence, and the Estonian government, indicates that Russia played a major role.[76] Only one person was arrested in the aftermath for conducting attacks from within the country. Allegedly this student was arrested because his origin of attack inside Estonia facilitated sufficient collection of evidence.[77] The Estonian government made formal requests to Russia for help in investigating the attacks, but was repeatedly denied.[78] In the years following the attacks, Estonia identified its weaknesses and addressed them to better deal with similar attacks in the future. The cyber-attacks uncovered legal and technical issues with which advanced nations had not yet dealt, particularly if such an attack amounted to an armed attack and could thereby invoke Article 5 of the NATO treaty permitting an allied response.[79]

---

72 Stiennon, *Surviving Cyber War*, 88.

73 Ottis, *7th European Conference on Information Warfare*, 2.

74 Stiennon, *Surviving Cyber War*, 88.

75 Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Washington, DC: IOS Press, 2009), 165.

76 Stiennon, *Surviving Cyber War*, 88.

77 Ottis, *7th European Conference on Information Warfare*, 3.

78 Ibid.

79 Christian Czosseck, Rain Ottis, and Anna-Maria Taliharm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic, and Organisational Changes in Cyber Security," in *The Proceedings of the 10th European Conference on Information Warfare and Security*, Academic Publications (2011): 57.

2. Proposed Causal Factors

a. Sophistication

Having discussed the background of the case study it is possible to examine some proposed causal factors that affected the level of impact of the cyber-attacks against Estonia. This analysis will help to determine the importance of certain causal factors in order to better understand the deterrent nature of offensive cyber-attacks. The sophistication of the attacks against Estonia is one variable that is worth examining. Although the scope of this attack was unparalleled in history, the specific tools used were relatively simplistic. DDOS was the predominant weapon of choice and was used against commercial banking and media as well as government websites.[80] As previously discussed, DDOS overwhelm a network with meaningless traffic and requests to the point where the network can no longer process them.[81] These attacks were simultaneously launched by hundreds to thousands of commandeered "zombie" computers.[82] The combined effects of the attack made further service for network patrons impossible. These types of attacks do not destroy systems, manipulate data, and they are relatively easy to fix although it may require complete disconnection of the network from the world, as was necessary by Estonian banks. More advanced SQL injections intended to hack and possibly manipulate data were also used and had limited success, although their success was in part limited by the low number of SQL attacks attempted.[83] There are many potential reasons that the attacks against Estonia were of low-level sophistication. Particularly plausible reasons are that the Russian government knew that the chances of their attribution increased with sophistication, the intent of the attacks on Estonia was not to destroy digital infrastructure, or that the attacks were essentially a "live-fire" exercise to determine and demonstrate weapon capacity and evaluate international reaction. The relatively low level of technical sophistication limited the destructive effectiveness of

---

80 Nazario, *The Virtual Battlefield*, 165.

81 Martin Libicki, *Conquest in Cyberspace* (New York: Cambridge University Press, 2007), 81.

82 African Network Information Center (AFNIC), "Estonia Cyber Attacks 2007," December 14, 2012, http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf, 11.

83 Ottis, *7th European Conference on Information Warfare*, 3.

these attacks. Networks were overwhelmed, websites defaced, and routers were damaged, but that was the extent of the damage.[84] What the attacks lacked in sophistication and destructive capacity however, was compensated for by a massive coordinated effort that made it possible to significantly affect almost all of the nation's citizens. Due to rapid response by Estonian officials, particularly of the Computer Emergency Response Team (CERT) the adverse effects of commercial and government service denials were limited and reversible. What remains important though is that a majority of the citizens of Estonia, to include the government, were aggressively and successfully attacked for over three weeks. While appropriate Estonian response and subsequent mitigation efforts helped address weaknesses, it is logical to surmise that their failure to do so could easily have eroded public confidence and support for the government.

b. State Dependency

State dependency on technology is a proposed casual factor worth examining because the degree of technological variance throughout the world could have implications for the level of impact of an offensive cyber-attack against a given country. Although it does not capture all aspects of a state's reliance on and employment of digital connectivity, the Internet's penetration rate, or ratio of Internet users in a society, does provide a rough metric to gauge potential vulnerability.[85] Estonia's reliance upon technology provided a significant vulnerability to any potential adversary that desired to avoid more conventional tools of diplomacy. By 2007, the Estonian digital infrastructure encompassed the functions of the government, power grid operations, financial services, and the water supply and distribution system. Additionally, 97 percent of banking transactions occurred online while over 60 percent of the population relied on the Internet to conduct their normal banking functions.[86] An IT director at the Estonian Defense Ministry explained that the Internet had pervaded their society to such a degree that their

84 AFNIC, "Estonia Cyber Attacks 2007," 17.

85 A brief discussion regarding the need for a better metric is in the concluding chapter.

86 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 53.

normal bureaucratic processes were referred to as a "paperless government."[87] In reference to their technological dependence Estonia has been jokingly referred to as "E-stonia."[88] Estonia's experience is a valuable case study because their technology infusion was ahead of its time and provides valuable, albeit painful, lessons for the majority of the developed nations that are following in its footprints. While cyberspace technology can provide many benefits in terms of efficiency, costs-savings, ease of use, and speed of information, it is imperative to also realize the vulnerabilities that are created. This is particularly true when the digital infrastructure is not designed to defend against low-level cyber-offensive weapons. Being the first victim of a large-scale cyber-attack, Estonia publicly demonstrated that the combination of Internet reliance and weak defense was dangerous. While their techno-savvy has been discussed, it is also important to highlight specific weaknesses that provided a vulnerable attack surface. Incorrectly configured webservers created a flaw by which the attackers could quickly overwhelm the websites, which was exacerbated by an infrastructure design that had numerous bottlenecks.[89, 90] Because Estonia suffered from a shortage of adequately trained Internet security professionals, countering the onslaught and addressing the damage required an allied CERT effort from Finland, Germany, Israel, Slovenia, the EU, and NATO.[91] While this considerable effort was largely due to the fact that an attack of this scale had never happened before, Estonia was nevertheless short-sighted their preparations. Had these issues been identified and addressed prior to the removal of the Bronze Statue, it is possible that the adversary's decision calculus would have realized that an offensive cyber-attack was not an effective tool of diplomacy.

---

87 Ibid.

88 Jamie Kitman, "President Ilves: the man who made E-stonia," *The Guardian*, last modified November 3, 2011. http://www.guardian.co.uk/world/2011/nov/03/president-ilves-made-estonia.

89 Stiennon, *Surviving Cyber War*, 87.

90 Estonian Information System's Authority, "Facts about Estonia," December 14, 2012, https://www.ria.ee/facts-about-e-estonia/.

91 Herzog, *Journal of Strategic Security*, 54.

c. Government Involvement

Although direct Russian involvement in the cyber-attacks was never positively proven, circumstantial evidence certainly seems to indicate that the nation played a major role. With the movement of a Russian monument as a triggering event, Russian involvement and cooperation appeared to escalate over the course of the attacks so much so that the President of Estonia publicly called for Russia to remain civilized.[92] Angry anti-Estonian rhetoric from the Russian media and senior state officials, to include President Putin and members of the Duma, certainly did not help assuage the attacks and likely fueled the fire.[93] Russian refusals to help Estonia investigate the attacks that originated in Russia, despite a signed treaty that called for such cooperation, are also evidence that Russia was trying to hide larger involvement.[94] While NATO did not directly accuse Russia, one official did say "I won't point fingers. But these things were not done by a few individuals. This clearly bore the hallmarks of something concerted."[95]

It is important to discuss the possibility of Russian involvement because attacks of this magnitude are unlikely without either direct or indirect support of a state sponsor. Their role in actually launching the attacks is too difficult to determine, but it is safe to say that Russia indirectly supported the attacks by repeatedly fueling a hostile situation in public, and possibly by proxy in chat rooms, and subsequently protecting attackers from investigation or punishment. A member of the Cooperative Cyber Defense Center of Excellence in Tallinn, which is a NATO organization created as a direct result of the attacks against Estonia, posited that the Russian government's involvement may have been as the coordinator of a *people's war* where the computer-savvy Russian citizens were manipulated by the government towards a common enemy.[96] It is an appealing strategy for the government because the lack of direct evidence provides plausible deniability, but the effects are nonetheless massed on the target. The veil of

---

92 Stiennon, *Surviving Cyber War*, 88.

93 Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, Last modified May 16, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

94 Ottis, *7th European Conference on Information Warfare*, 3.

95 Herzog, *Journal of Strategic Security*, 53.

96 Ottis, *7th European Conference on Information Warfare*, 3.

secrecy and protection provided by the Russian government is also an important factor in the lingering effects and ambiguity that resulted from the Estonian attacks. Only a state actor has the ability to stonewall international calls for an investigation. In terms of level of impact, the fact that there was a twenty-two day long cyber-attack and the attacker could not be confirmed or brought to justice certainly had an effect on the psychology and confidence of the Estonian government and citizens. It likely also sent a very clear message to states around the world that possessed burgeoning offensive cyber-weapons resources and were trying to think through the impacts of their employment. Not only was it possible to coordinate masses of "hacktivists" to execute cyber-attacks against a common target, but subsequent refusal to cooperate with investigations provided an additional layer of deniability. If there is no investigation, then culprits will not be identified. It is safe to say that had the Russian government handled the situation by purely diplomatic means rather than rabble-rousing and inciting the masses, then the cyber-attacks against Estonia would have been much less significant in both immediate and long-term effects.

3. Value of Dependent Variable

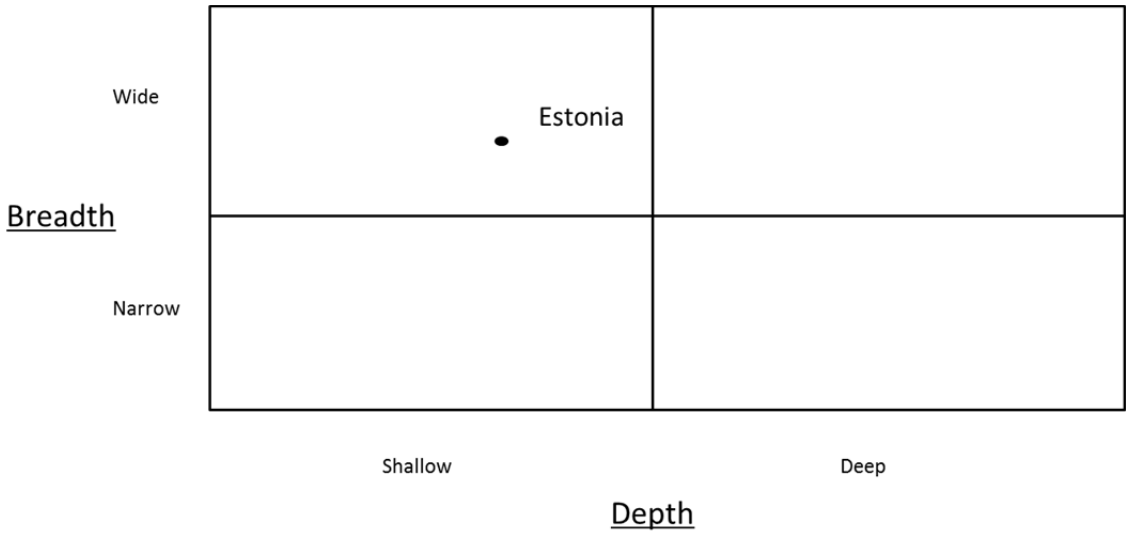

Figure 3. Effectiveness of Cyber-attacks Against Estonia

Available evidence indicates that the level of impact of the offensive cyber-attacks on Estonia is in the upper-left quadrant (Figure 3). In terms of breadth, the target was very widespread as the government, banking, and media were victim to the attacks. Although these services were critical to the daily lives of the citizens, the attack did not target other vulnerabilities that could truly have crippled the nation such as the power, sewer, and air traffic control services. Had these additional targets also been attacked the breadth of the attacks would have been assessed to be near the maximum value.The attacks against Estonia remained shallow in depth because the predominance of attack techniques was DDOS and web defacement conducted by botnets or recruited "hacktivists." Although there were occasional SQL injections that were much more sophisticated, the attacks only temporarily prevented citizens from accessing certain government and financial services while also subjecting them to digitally-delivered propaganda. There was no evidence of truly destructive software that caused physical damage, loss of data, or irreversible consequences. This absence limited the effective depth of the attack.

4. Conclusion

This case study provides several valuable points that shed light on the role between the proposed causal variables and the attack's level of impact. In terms of the attack's sophistication, this proposed causal factor limited the depth, but allowed for increased breadth. The intended depth of the attack may have been shallow in order for the aggressor to remain anonymous or perhaps a shallow attack achieved the intended effects. Regardless however, the sophistication of the attacks limited the level of impact specifically in terms of depth. While the occasional SQL injection did increase the depth value of this case study, the preponderance of DDOS and defacements were largely a result of unsophisticated techniques. While the relative unsophistication prevented a truly deep attack, it is also important to note that the Estonians' lack of preparedness and adequate defenses against DDOS attacks did contribute to the depth that the attacks did reach. The Estonian government had to request CERT help from more defensively-prepared nations in order to counter the onslaught of the botnet attacks. Additionally, the depth of the attack was limited when the Estonian government essentially unplugged its

digital connection to the outside world, and although this action limited the effectiveness of the attack, it still caused massive disruption to the many customers of Estonian banks that were outside of the country.

State dependency did play a factor in the level of impact, but it was mainly in terms of the breadth of the attack. Estonia's well-documented digital integration created a vulnerability that was easily targeted. Because an overwhelming majority of the population used the Internet for financial transactions, communication and information sharing, and to access government services, to include voting, the attacking force had several targets from which to choose. Had the primary targets required a level of sophistication that the aggressing state was not willing to employ, the abundance of targets meant the attackers merely had to keep looking until they found adequate vulnerabilities. In a state with limited dependency, there are two issues that will limit the impact of the attack. First, the number and variety of targets will be severely more restricted than in a digitally robust society. Secondly, because a minority of the citizens relies on digital services, an attack on a given sector will affect a much smaller percentage of the citizens than was the case in Estonia.

Although state role remains unproven, evidence indicates that state involvement was necessary for this caliber of offensive cyber-attack. While the intent is not to uncover the aggressor's identity, it is important to highlight the ability of a state-level entity to use national-level pulpits to incite public anger against a common enemy, employ chat-rooms and blogs to provide specific code and targets to attack, and then stonewall any international attempts to attribute responsibility. Without concrete evidence it is necessary to draw some conclusions based upon what can reasonably be assumed. The state's involvement presumably included determining the breadth and depth of the attack before it began and subsequently monitoring the situation to make sure that it did not escape the designated boundaries. Because a shallow depth leaves a less traceable fingerprint on the attack, the state likely limited the sophistication of the attack to DDOS and defacement. In order to compensate for an unwillingness to launch a deeply destructive attack, the state increased the breadth by sponsoring a massive coordination

effort to mobilize a "hacktivist" army. This call to arms was conducted on Russian blogs and chat-rooms and provided specific targets and attack codes. The breadth increased the effectiveness of the attack while providing the state with two advantages. First, the attacks were not of such great breadth that would likely instigate international military response, so the state had the opportunity to monitor and test the international opinion to their actions without being in legitimate danger. The second advantage was that these broad and outsourced attacks gave the state the opportunity to test its command and control of such an operation and make improvements for use in future conflicts.

C. CASE STUDY 2: GEORGIA

1. Overview

Georgia is a former member of the Soviet Socialist Republics, and as such, has experienced significant turbulence since its dissolution. The turmoil actually reaches much further into history as their governing entities changed frequently between the Russian czars, short-lived independence after the Bolshevik Revolution, the Soviet Union throughout the Cold War, and again to independence following the Soviet Union's collapse in 1991. Georgia's post-independence borders include South Ossetia, which is a region that contains people ethnically and linguistically different from Georgia.[97] The region of North Ossetia is within the borders of the Russian Federation although its inhabitants are ethnically the same as the South Ossetians. Violent turmoil has been the state of the relationship between South Ossetia and the Georgian government since 1990 with various attempts by a Russian-backed South Ossetia to gain autonomy and several violent suppressions by the Georgian government. The situation continued to escalate after the 2003 election of Georgian president Mikheil Saakashvili who executed an agenda that saw significant military buildup, application to NATO, and increased aggression to quell the uprisings in the breakaway regions of South Ossetia and Abkhazia.[98] Russian opposition to all of Saakashvili's actions bolstered the rising

---

[97] Herzog, *Journal of Strategic Security*, 95–6.

[98] Armed Forces Communications and Electronics Association (AFCEA), "The Russo-Georgian War 2008: The Role of Cyber Attacks in the Conflict," last modified May 24, 2012, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf, 3–4.

tension between the two states and emboldened anti-Georgian resistance by South Ossetia. Citing alleged ceasefire violations by South Ossetia, Georgia moved their military forces into the rebellious region on 7 August 2008 which sparked Russian military mobilization into South Ossetia where they launched air strikes against selected targets in Georgia.[99] What immediately preceded, and then continued throughout the Russian military action, but was never attributed to Russia, was an offensive cyber-attack against select portions of the Georgian digital infrastructure intended to confuse a coordinated military response, undermine the effectiveness of the Georgian government in dealing with such an attack, affect exported information about the war, and exacerbate the confusion of the Georgian citizens.[100] In an effort to influence how the international audience viewed the Russian actions, not only did hackers attack the BBC and CNN to prevent portrayal of the attack, but also massed efforts on some prominent online polls, such as CNN, to make it look like Russia was not the aggressor.[101] These rigged polls then further encouraged commentators to spin the situation in Russia's favor. Additionally, some of the cyber-attacks specifically attempted to incite and demoralize the Georgian people by defacing numerous websites with pictures comparing Mikheil Saakashvili to Adolf Hitler.[102]

Initial cyber-attacks targeted designated government and media services in order to prevent effective communication of the Russian invasion. As the Russian military movement into South Ossetia continued, the cyber-attacks were expanded to include additional government sites, financial institutions, media outlets, businesses, educational institutions, as well as known Georgian hacking forums in an effort to limit a cyber-counter-response.[103] Russian hackers also allegedly attacked servers in countries, such as Turkey and Ukraine that provided critical communication services to Georgia so as to

---

99 Herzog, *Journal of Strategic Security*, 95–6.

100 AFCEA, The Russo-Georgian War 2008, 6.

101 Ibid., 10.

102 Ibid., 9.

103 John Bumgarner and Scott Borg, *Overview by the U.S.-CCU of the Cyber Campaign Against Georgia in August of 2008*, special report (Boston: United States Cyber Consequences Unit, 2009), 5–6.

further disrupt communication.[104] The kinds of cyber-attacks that accompanied the Russian military intrusion were not particularly sophisticated and were mainly either DDOS attacks or web-defacements. Attacks intended to cause physical damage were not perpetrated by the hackers although these targets were certainly vulnerable.[105] Although cyber-attacks continued for several weeks afterwards, the majority in both numbers and effectiveness took place during the same five day window of the Russian military actions between 8 and 12 August 2008 when a ceasefire agreement was signed. Specific attribution was never established although evidence indicates a wide variety of Russian entities were possibly involved in the attacks to include the Russian military, powerful business networks, Russian organized crime, intelligence agencies, and patriotic Russian hackers.[106]

The Georgian response specific to the cyber-attacks was guided by inadequate defense and preparation. Fortunately for Georgia, Estonia had recently suffered a very similar attack and was able to provide assistance in limiting the amount of damage done and addressing additional vulnerabilities. Initial and rudimentary tactics such as blocking IP addresses of Russian origin worked for only a short-time as the attackers easily rerouted their attacks. In a fortunate and innovative turn for the Georgian government, executives from several large web server companies such as Google and Tulip allowed critical government functions to be transferred to their servers in the United States. Although this action did help to alleviate the direct attacks on Georgian systems, it did redirect a significant volume of attacks against servers in the United States and consequently spark academic debates about private companies and their role in cyber-conflict. Georgian nationalist hackers did rally in support of their nation and attempt DDOS counter-attacks against news media and other select targets, but their efforts were largely ineffective and unnoticed in comparison to the volume of Russian-based cyber-attacks.[107]

---

104 AFCEA, The Russo-Georgian War 2008, 8–9.

105 Bumgarner and Borg, *Overview by the U.S.-CCU* , 4–5.

106 AFCEA, The Russo-Georgian War 2008, 13.

107 AFCEA, The Russo-Georgian War 2008, 12.

2. Proposed Causal Factors

a. Sophistication

The sophistication of the attacks against Georgia was relatively unremarkable with DDOS and web defacement being the primary tools of cyber-attack. While these tools are both relatively simple in concept and execution, the method of their employment indicated a much higher sophistication. As previously discussed, DDOS attacks overwhelm the capacity of a network or computer to accept and reply to all of the requests thereby causing it to crash and be unable to provide further service. These attacks are generally executed by large numbers of networked computers, sometimes unknown to the owners, under the command and control of a "bot master" that remotely coordinates them to conduct massed attacks. Evidence from the Georgian attacks indicates DDOS software had been developed and implemented specifically for use against the Georgian networks. Some of the denial-of-service attacks were carried out by software normally intended to evaluate the stress potential of a network, while even more advanced software targeted websites and requested non-existent web pages. The targeted websites then endlessly looked for nonexistent web pages which quickly incapacitated server capability.[108] Although the weapons of choice were DDOS and web defacements, certain more advanced attacks used SQL injection, which allowed much more experienced hackers to accomplish DDOS-like effects without the number of networked zombie computers. These techniques permitted the attacking force to mount their attacks with less zombie computers while still creating enormous amounts of traffic. While much of the specific attack data is not publicly available or attainable, an analysis firm called Arbor Networks released some statistics that demonstrate the nature of some of the more significant denial-of-service attacks. Their data reveals that the attacks averaged an intensity of 211.66 Mbps with a peak of 814.33 Mbps with an average duration of 2 hours and 15 minutes and a 6 hour maximum duration.[109] This level of traffic can be handled by appropriate hardware, but thanks to the stress test software used by the Russian

---

[108] Bumgarner and Borg, *Overview by the U.S.-CCU* , 4–5.

[109] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, special report (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2008), 9.

attackers, they were able to determine exactly the level of traffic necessary to incapacitate the Georgian infrastructure. It was also fortuitous that the Georgian commercial and government digital infrastructure was completely unprepared to defend against an attack of this scale.

Although the attack tools were used in a more sophisticated manner than in previous cyber conflicts, such as Estonia, they were still relatively basic compared to the arsenal of cyber-weapons that could have potentially been used. But because denial of service and defacement were the intended effects, these tools were the logical weapons of choice. In order to increase the level of traffic levied against Georgian servers and websites, Russian hacking and blogging forums were employed to recruit a "hacktivist" army. These websites posted the scripts, tools, and instructions necessary for their execution, but also provided a list of 36 different websites against which the recruited hackers should launch their attacks.[110]

An important point to take away from the Georgian cyber-attacks is that unsophisticated tools were sufficient to accomplish the intended effect of preventing government coordination and to a limited degree demoralizing the population. There were stronger cyber-tools available that could have caused significant physical damage and much more debilitating effects to the digital infrastructure, but the aggressor force likely imposed self-restraint so as not to induce strong international opposition and investigation. By massing the unsophisticated, but debilitating effects using recruited hackers and altered software, the aggressor force was able to shut down key government and business online ability while retaining their veil of secrecy.

b. State Dependency

There are many commonalities between the offensive cyber-attacks launched against both Estonia and Georgia, but state dependency on and the integration of a robust digital infrastructure are vastly different between the two states. 2007 statistics indicate that there were approximately 8.3 Internet users per 100 people, which puts Georgia roughly in the same ballpark as nations such as Haiti and Tanzania. By

110 Tikk et al., *Cyber Attacks Against Georgia,* 10.

contrast, Estonia and the United States had 66.2 and 75.3, respectively.[111] Most of the Internet use is among business and government professionals as it has not permeated into the regular daily life of the citizenry as it had in many more technologically advanced nations. In terms of Georgia's dependence upon other nations for connectivity, post-conflict investigations indicate that a majority of the nation's over-land Internet connections go through Russia while most of the Internet traffic is routed through Turkey (and then Russia) before being sent to its final destination. Georgia was working to decrease their dependence upon traditionally adversarial states by routing fiber optic cable through the Black Sea and into Bulgaria, but that project had not yet been completed before they were victim to the 2008 cyber-attacks.[112] An additional aspect of dependence was that 90 percent of the Georgia's commercial services were controlled by Caucasus Network Tbilisi, a company whose infrastructure was in the middle of the conventional military action and thereby suffered debilitating damage.[113]

The average citizen's lack of dependency on Internet connectivity vastly decreased the attack surface vulnerable to attack which thereby limited the effectiveness of the attack. Because most citizens did not conduct online business transactions, obtain their news from the Internet, or use online government services their daily life was not vastly different than had there not been an offensive cyber-attack. This was not true of the government and business sectors in Georgia where a majority of the connectivity resided. Because the attacks were successful in denial-of-services on government websites, communications, and news media, the attacks effectively crippled the ability of the government to coordinate their response, present their story to the international world, and inform their people. While a majority of people were not directly reliant on the Internet, the crippling of government and news media prevented information flow from the capital to regional news and government centers. While this obviously affected the

111 The World Bank, "Internet Users (per 100 people): 2007" January 12, 2012, http://data.worldbank.org/indicator/IT.NET.USER.P2?page=1.

112 Tikk et al., *Cyber Attacks Against Georgia,* 6.

113 Ibid., 14.

citizens' ability to remain abreast of the situation, it also had a demoralizing effect in that connected citizens and media could not access their government in a time of war.[114]

There are several key points drawn from the level of Georgian dependency on connectivity. First, the fact that a minority of the population relied on the Internet in the course of their daily lives limited the impact of the attack on the private sector. Unlike in Estonia, a majority of the Georgian people did not conduct banking or depend on web-based government services. A second point is that the Georgian commercial and governmental burgeoning integration of Internet-based technology made this an area vulnerable to attack. This is particularly true in light of the fact that the nation was inadequately prepared to defend against or counter the cyber-attack. A third point deals with the structure of the national dependency. With one company providing 90 percent of the services and a majority of the over-land cables providing connectivity going through an established adversary, Russia, the Georgian government lacked the diversity of connectivity that is necessary to continue continued operations. Not only were their eggs all in one basket, but the source of the eggs was an enemy. Individually those issues are significant enough to create a very attractive attack surface. Georgia was very fortunate that Google, Tulip Systems Incorporated, Poland, and others came to their aid and hosted critical government and media services on servers that were outside of Georgia, but developing government cyber-conflict policy and laws will likely prevent this from being a common course of action in future cyber-conflicts.[115] The final point taken from the investigation of NATO's Cooperative Cyber Defense Center of Excellence, which was created in response to the Estonian attacks, states that nations with low dependency on Internet connectivity and IT often suffer the most in terms of their ability to efficiently push information.[116] One reason is that a robust digital infrastructure makes communication much more efficient. The other possible explanation is that when a state relies on limited conduits with little redundancy, any disturbance to service can have disproportionate effects.

---

[114] Ibid., 14–15.

[115] Ibid., 14.

[116] Ibid., 16.

c. Government Involvement

Investigations of the cyber-attacks against Georgia failed in the attribution attempts, but like the Estonian case study, an overwhelming preponderance of evidence implicates Russian involvement. One of the more peculiar aspects of the cyber-attacks was the precise timeline that it followed compared to the conventional military action by Russia. On 19 July, three weeks before the attacks started, network monitoring services witnessed a DDOS attack against the website of the Georgian president as well as the presence of a command and control server typically used to coordinate botnet attacks. The type of command and control server was known to be one used by Russia.[117] This preliminary attack on the president's website lasted 24 hours before the site was moved to the United States, and the command and control server went offline shortly thereafter and did not come back online until 8 August when the massive cyber-attacks began. Evidence indicates that in the three weeks prior to 8 August the attackers were performing reconnaissance and coordinating their botnets in anticipation of a massive cyber-onslaught when Russia became kinetically involved.[118] In the hours prior to Russian commencement of military activities, cyber-attacks successfully gained control of state computer servers and incapacitated the Georgian government's ability to either effectively coordinate their attacks or communicate with the outside world. The Georgian Ministry of Foreign Affairs immediately fingered Russia in a statement given on their website, which was now being hosted by Google, saying that "a cyber-warfare campaign by Russia is seriously disrupting many Georgian websites."[119] What is also remarkable is that many of the attacks were specifically designed for use against Georgia and were developed in some cases years in advance. Some of the DDOS software previously discussed was designed specifically for the Georgian infrastructure, while the intricacy of certain defacement material indicates that it had been developed at least two years prior to the start of the 2008 Russo-Georgian war and by an entity familiar with psychological

117 Ibid., 12.

118 AFCEA, The Russo-Georgian War 2008, 6.

119 Tikk et al., *Cyber Attacks Against Georgia,* 37.

operations.[120] It is not reasonable to think that a private citizen hacker would years in advance develop weapons specifically intended for use against Georgia without a government request or sanction. Developing weapons for use against potential state adversaries is the business of the government, regardless of whether they develop it themselves or outsource it.

Not only did circumstantial evidence indicate some measure of Russian involvement, but investigations into the event uncovered direct links to Russian organized crime, specifically the Russian Business Network (RBN) which is a well-known perpetrator of cyber-crime. Many of the servers used to attack the Georgian infrastructure were traced to criminal organizations such as RBN and network monitoring services even witnessed these servers simultaneously executing criminal attacks against unrelated targets.[121] Two points indicate that these organizations were acting at the behest of a larger entity such as the Russian government. Like the recruited "hacktivist" groups organized on the hacking forums, large criminal organizations have little interest in targeting government and communications servers of a state-entity, particularly when their normal criminal enterprises are so lucrative. Additionally, there have been several allegations that the Russian government regularly uses criminal organizations to carry out actions that are too delicate if the actions were to be attributed to the state.[122]

While the direct involvement of the Russian government has yet to be proven, circumstantial evidence regarding the government's affiliation is strong enough to form some initial conclusions. The nested timeline, complete with prior notification of Russian military action, seems to indicate that the government was certainly involved. While it may not have been government personnel or computers conducting the attacks, overwhelming evidence supports that Russia served as the puppet-master behind the cyber-onslaught. Much as was the case in Estonia, the government likely either directly oversaw or sanctioned deliberate preparations such as the recruitment of able bot masters with sufficient zombie armies, distribution of malicious code with intended targets,

120 AFCEA, The Russo-Georgian War 2008, 9.

121 Bumgarner and Borg, *Overview by the U.S.-CCU* , 4–5.

122 AFCEA, The Russo-Georgian War 2008, 17.

development of psychologically effective defacement campaigns, and coordinated approval for the cyber-attacks to commence. All of these activities could be surreptitiously performed so that traceable ties and incrimination of government sources were nearly impossible after the fact. While a bot master or criminal organization could have launched piecemeal attacks, but it took a state entity to recruit and bring all elements together and concentrate their effects at the decisive time and place.

3. Level of Dependent Variable

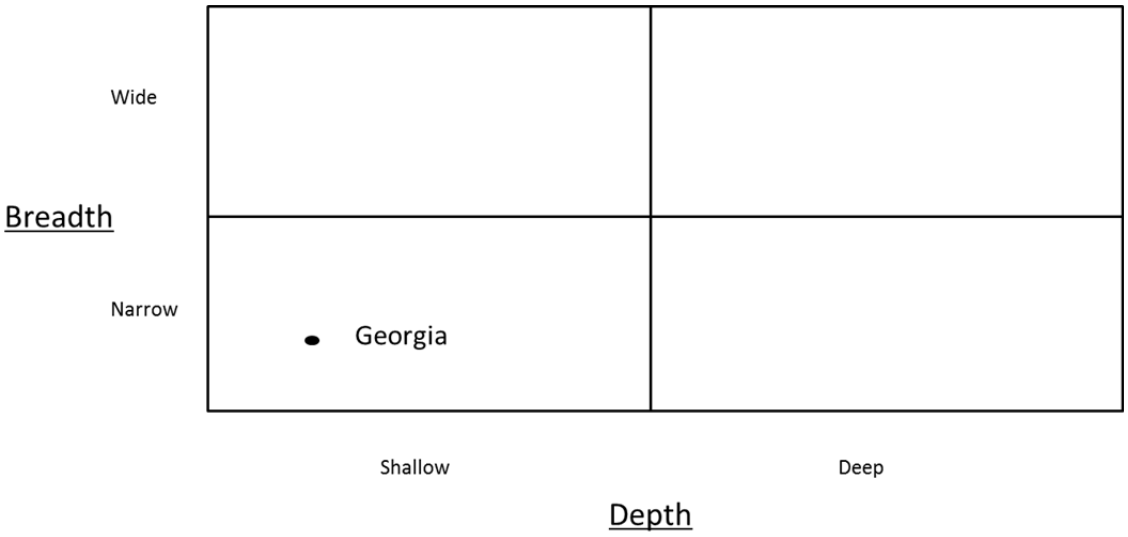

Figure 4. Effectiveness of Cyber-attacks Against Georgia

Available evidence indicates that the offensive cyber-attacks launched against the nation of Georgia were both shallow and narrow, thereby placing it in the lower-left quadrant (Figure 4). The breadth of the attack was narrow as the primary targets were government websites and media. Although the Georgian digital infrastructure was considerably less robust than that of Estonia, there remained additional sectors that were left untargeted, presumably because attacking them would not have contributed to the aggressor's seemingly military objective. The depth of the attack was relatively shallow as the primary effects were denial of service and defacement. The denial of service was designed to limit the Georgian government's ability to communicate with the outside world or to effectively coordinate its military response, while the defacements were

intended to introduce incendiary propaganda. These attacks were extremely successful, but only to the limited shallow depths to which that they were intended to reach. Significant disruption, destruction, or alteration of data was neither present in this attack, nor necessary to accomplish the objectives.

4. Conclusions

The cyber-attacks conducted against Georgia help to further develop the role played by the proposed causal factors in determining the level of impact. When viewed against the backdrop of what was technologically possible, the sophistication of these attacks was unremarkable. DDOS and web-defacements were again the primary tools which thereby severely limited the depth of the attacks. There is evidence of occasional use of SQL injection, but this technique was uncommonly altered to produce DDOS-like effects rather than the more destructive effects that it is capable of producing. And although unsophisticated in nature, the depth reached by the cyber-attacks was again augmented by the totally inadequate preparation of the Georgian government to defend against such an event. The Georgian government had to employ NATO CERT teams and accept various international offers to host critical government web services in order to alleviate the effects of the cyber-attacks. The Estonian incident was only a year old and the lessons-learned from that event had not widely taken root, particularly to nations with limited dependence on Internet connectivity. Although the simplicity of DDOS contributes to its allure and success as a cyber-weapon, more defensively prepared nations would not have so easily succumbed to these attacks.

Aspects of Georgian digital dependency offer some very valuable insight towards how this factor affects the level of impact. First, the non-dependence of the average Georgian citizen reduced the breadth of the vulnerable attack surface available to the aggressor. While this could arguably be one reason for the limited breadth of the attack against Georgia, it seems more plausible that their non-reliance is coincidental to the narrow breadth as the objectives of the attack did not require a more expansive breadth. The point is worth noting that reduced dependence does reduce the breadth of an attack, but if the objectives can be met by a narrow attack, then the level of the state dependency

is not important. The second point about state dependency highlighted by this case study is that the depth of an attack can be exacerbated by a high dependency on assets that have limited diversity. One company controlled over 90 percent of the nation's commercial traffic, while most of the physical lines providing connectivity ran through the territory of Georgia's most dangerous enemy.[123] Both of these factors intensified the depth of the cyber-attacks as Georgia was unable to unilaterally overcome the effects created by this dependency. They were indeed fortunate for the assistance of several foreign governments and commercial enterprises.

The offensive cyber-attacks against Georgia were never positively attributed to the aggressor, although circumstantial evidence overwhelming indicated heavy Russian involvement. Using their involvement as an assumption, several points can be extracted from this case study regarding the effect that state involvement has on a cyber-attack's level of impact. The depth of the attack was directly affected by the creation of a digital cyber-militia that used relatively simple attack methods. Much as a hastily recruited conventional militia is generally incapable of complex military operations, the cyber-militia used in this attack also had limited capability. The aggressing entity understood this fact, but likely concluded that increased depth carried a pronounced risk of their implication. This is an important point to make because although governments have the ability to greatly increase the depth of attack, their involvement generally limits the depth in fear of reprisals. State involvement also directly impacted the breadth of the attack by their provision of a list of websites for their cyber-militia to target. These targets consisted mainly of government and media websites and the target list was posted in several blogging and chat-room websites. By viewing the government's role as similar to that of a marionette, it is not difficult to imagine the breadth of the attack being much wider had a larger variety of targets been supplied. The reason for the restraint it difficult to attribute, but the most probable reasons are that the narrow attacks met the larger operational objectives and the very narrow attack carried less risk of external condemnation.

123 Tikk et al., *Cyber Attacks Against Georgia,* 6,14.

A final point regarding government involvement applies to both the breadth and depth of the attack. The succinct coordination between conventional military and cyber-operations allowed for an attack of limited depth and breadth to be successful. Because the effects of the attack were perfectly synchronized with conventional military operations, the aggressing state did not need to introduce more powerful cyber-attacks with more lasting effects. This synchronization facilitated a minimal use of cyber-force and thereby reduced the risk to positive attribution or aggressive adverse international response.

D. CASE STUDY CONCLUSIONS

Before discussing the conclusions induced from the case studies it is important to mention that they were limited in the scope of what they could examine. There are three reasons for this. First, because the advent of cyber-weapons has really only been significant in the last two decades there are a limited number of cases from which to choose. Secondly, of the available case studies there is normally a very limited amount of information that is released. The aggressor state has obvious reasons for not releasing the information, while the targeted state does not generally desire to elaborate upon their vulnerabilities. The third limiting factor of these case studies was self-imposed. In order to extract as much valuable information as possible from the case studies it was necessary to limit the range of certain variables, specifically the intent of the aggressing state.[124] With the intent fixed as seeking to subvert the ability of the government to successfully protect and provide services for their citizens, the two most prominent case studies were the cyber-attacks against Estonia and Georgia. It is also important to mention that both of these attacks were allegedly perpetrated by Russia, but this was a difficult coincidence to avoid in such a narrow field of potential case studies.[125]

The case studies revealed several important insights into the influence that proposed causal factors had on the cyber-attack's level of effectiveness. The proposed causal factors examined throughout these case studies were the sophistication of the

[124] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 31.

[125] Ibid.

cyber-weapons, the targeted state's level of dependency, and the level of the aggressor state's government involvement. The most important point to make is that government involvement in these cases was never proven, so their role is alleged but supported by very strong circumstantial evidence. That being said, the government's involvement in each of the case studies played the largest role in determining the ultimate level of the attack's effectiveness. Evidence examined in the research indicates that Russia was the driving force behind each attack and exerted their influence by recruiting an outsourced cyber-militia, providing lists of targets, and coordinating the timeline of the attacks. Russia's recruitment of a cyber-militia by making inflammatory public statements against their enemies or more active recruitment in blogs and chat-rooms is an essential point to examine because it could very easily serve as a common practice of other aggressor states. The benefit of this practice is that it provides the aggressor state with plausible deniability. A state can easily serve as the ignition to tinder without demonstrating clear violation of any international law. The pulpit serves as a way to incite the cyber-militia, while blogs and chat-rooms provide the anonymity and outlet for the government to exercise limited control and coordination. The price of this plausible deniability is that the state sacrifices their direct control of the operation, and specifically the level of destruction that is possible. By recruiting an online cyber-militia, the state essentially relegates itself to the tools and common practices of hackers such as DDOS, SQL attacks, and website defacement. Russia certainly has a very advanced and destructive cyber-weapons capability and could have conducted attacks of much greater severity than actually took place in Estonia and Georgia, but this comes with a higher risk of attribution. Non-state entities do not typically have the resources, skill, or protection necessary to execute cyber-attacks that are both wide and deep, so it is likely that use of weapons of this caliber would lead to increased risk to the state.[126] This increases the risk because wide and deep attacks would require weapons that only states possess, thereby increasing their risk of attribution. Additionally, very destructive attacks would likely invite more aggressive international opposition and investigation. There are two main points to take away from this discussion of state involvement. The first point is that there

[126] Herzog, *Journal of Strategic Security*, 53.

is a tradeoff between level of effectiveness of a cyber-attack and a state's ability to retain plausible deniability. The second point derived from the case study research is that state involvement limits that the effectiveness of a cyber-attack in both its depth and breadth. Although some states possess advanced cyber-weapons, the risks associated with their employment are great. The intent of the aggressor state in these case studies did not warrant assuming that risk, but cyber-attacks such as Stuxnet demonstrate that is not always the case. It is worth noting that the corollary of this argument is that non-state actors that acquire destructive cyber-weapon technology could pose a very serious threat.

Sophistication of the weapons employed did affect the depth and breadth of the attacks. Because the cyber-weapons employed were mainly individual hackers and botnet armies, the ability to deeply affect the target's digital infrastructure was not possible. Appropriation of slave computers by bot-masters to carry out DDOS attacks allowed for a much wider breadth than would have been possible had the attack relied solely on the willing recruitment of hackers. But as a causal factor, the research indicates that the level of sophistication was mainly a result of government involvement. So, while the weapon sophistication does affect the effectiveness of the attack, it must be noted that the level of sophistication is largely a result of state participation. The point to take away from this discussion is that highly sophisticated weapons are not necessary to have an effect. Large numbers of unsuspecting computers can greatly increase the breadth of an attack, as can large and coordinated groups of self-taught computer operators that can follow instructions. Both of these options offer several advantages to complex weapons, mainly that they are cheaper and protect plausible deniability. However, not all targets are susceptible to broad, but shallow attacks and may require use of much more sophisticated cyber-weapons. An attack on a SCADA or satellite guidance system, for example, would require a deep and narrow attack.

The last proposed causal variable, state dependency, was also instrumental in determining the effectiveness of a cyber-attack. There are several points that were revealed in the course of the case studies that are worth mentioning. One of the more apparent conclusions is that the target state's dependency upon digital connectivity can facilitate a broader cyber-attack, which in turn increases the level of effectiveness. The

high degree of the Estonian population's reliance provided a rich target field. It was not difficult for Russia to find vulnerabilities to attack, whereas the target field in Georgia was significantly more selective. This limited availability of targets consequently decreased the breadth of the attacks, and because depth was not increased in compensation, the overall effectiveness.

There are a couple other points to make about the state's dependency as a causal variable. State dependency plays a more important role in increasing the effectiveness when the aggressor's intent can be met by executing broad attacks. There were several ways to achieve the intended end-state of subverting the government's ability to protect and provide services to its people, one of which could be accomplished by a relatively easy and cheap attack on the availability of digital services. Russia did not need to deeply affect a target in either case in order to achieve their goals. Broad attacks against an Estonian society with very high reliance upon the Internet did alter the conveniences of daily life for several weeks, but that was essentially the limit of the damage. The attack on Georgia also required limited depth as the goals were to prevent internal and external communication to coordinate the government's response to Russian military operations. Had either scenario called for extremely narrow and specific targeting of a capability then the state's dependence upon networked technology would be irrelevant. The only thing that matters in that narrow case is whether that asset can be reached by the available arsenal of cyber-weapons.

Through their cyber-attack on Georgia, Russia also demonstrated that a high degree of reliance on digital technology by the population is not essential to execute a successful attack. As long as there is some variant of reliance and vulnerability that the aggressor can target then a state is in danger of falling victim to an attack. In both of the case studies government use of the Internet coupled with a lack of preparedness to defend their networks created critical vulnerabilities. Although lower Georgian reliance reduced the effectiveness of the attacks, it is important to note that the attacks were still executed effectively.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

Advances in cyber-technology over the past decades have given rise to the use of computer attacks as an effective weapon in conflictual relations between states. This research intended to refine some of the characteristics of this weapon's employment and draw some initial conclusions that provide insight into the role it plays in conflictual relationships. It was first necessary to establish a common framework by which to conduct this research.[127] This included exploring the assumptions and characteristics of traditional structural realist theory, examining a game theoretical model that demonstrates how states interact, and creating a list of attributes that help measure and describe the role that selected weapons have on interaction between states in this environment. The attribute framework was then applied to selected instances of offensive cyber-weapons. Of the attribute categories, the research focused on three factors and examined their role in determining the level of effectiveness of offensive cyber-attacks in Estonia in 2007 and Georgia in 2008. The case study conclusion provided refined analysis on the relationship between the proposed causal factors and an attack's level of effectiveness and extracted the trends that are relevant to understanding the construct of similar instances of cyber-conflict.[128] The last chapter of the research comments on the role of offensive cyber-weapons in the arsenal of tools of interaction between states. Provided also are some additional considerations and recommendations drawn from the case studies that are important to highlight, but did not relate specifically to the relationship between the selected causal factors and the level of effectiveness. Recommendations for further research is the last section and aims to focus research efforts towards issues that further the understanding of the causal mechanics of offensive cyber-attacks.

A. CYBER-WEAPON ATTRIBUTES

The case studies provided an opportunity to examine the causal role of selected factors on determining the level of effectiveness of an offensive cyber-attack.

---

[127] Goertz, *Social Science Concepts: A User's Guide* , 35.

[128] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 123-4.

The case study conclusions summarized the refined and nuanced influence of the selected factors. There were additional items of interest that arose throughout the case studies that could be of particular importance to those developing policy on the use of cyber-weapons. Some of the considerations are recommendations based upon non-causal factor trends that were identified through the course of the case studies, while other considerations are valid, but research is too premature to identify and suggest a course of action. The intent of citing those issues is to identify subjects that are very relevant to cyber-policy but that need more refinement.

Although only three specific proposed factors were examined, this research did shed light on additional attributes of cyber-weapons as a tool of diplomacy in conflictual relations between states. The potential destructiveness of the weapons is immense, but largely determined by the intended effects, employed technology, and level of state involvement. Unpredictable collateral damage imposed by the attack is largely dependent upon its depth. For example, a power distribution interruption suffered by ten million people for 30 minutes (narrow and shallow) is likely to incur less unpredictable collateral damage than a similar attack that destroys transformers and electrical control networks (narrow and deep). The deeper attack inhibits power distribution for an unknown amount of time and creates the environment for development of second and third-order effects. Comments made by a NATO spokesman following the attack on Estonia indicate that state control of cyber-weapons is high.[129] It is important to understand that individual hackers and criminal organizations do have their own limited arsenals of cyber-weapons, and that the NATO spokesman's comments imply that state control is necessary to provide either the planning and coordination effort or the weaponry necessary to be effective in a cyber-attack on a state-level scale.

Plausible deniability and covert use are two of the most troublesome characteristics of offensive cyber-weapons because they complicate the understanding of roles between the actors in conflict. Largely as a result of these aspects, the case studies demonstrate that the deterrent capabilities of cyber-weapons are not as well defined as

[129] Herzog, *Journal of Strategic Security*, 53.

those of the traditional tools of interaction. Understanding the interaction between states within the traditional realist framework becomes very difficult when actors can secretly employ weapons, and more importantly, plausibly deny the origin of use. In the cases of Estonia and Georgia, the inability to forensically attribute the attacks allowed the aggressor state, presumably Russia, to avoid any punitive action. The increasing concern in America regarding the Chinese role in cyber-espionage and theft of billions of dollars of economic and intellectual property, all behind the veil of plausible deniability, demonstrates the immediate relevancy of this issue.[130] Plausible deniability was not possible when using conventional military action or nuclear weapons. RMA-enhanced weapons increased covert employment, reduced collateral damage, and allowed for surgical precision, but still did not provide non-attribution capability. The capacity for cyber-weapons to be used by states without attribution is an issue that will continue to complicate state interaction in a conflict until this capability is either defeated by advances in cyber-forensics or thwarted by policy. This will be further examined in the subsequent section on policy recommendations. One last point regarding covert employment and plausible deniability is that that these characteristics of cyber-weapons create a better opportunity for the targeted state to create false perceptions regarding the effects. Although propaganda spins the effects of all tools of interaction, the difficulty in attributing cyber-weapon use makes it easier for the targeted state to manipulate the narrative and popular perception of an offensive cyber-attack regardless of reality.

Contestability of cyber-weapons adds an interesting element to the relationship between states. Conventional military action is contestable in that states can reasonably believe that they possess the ability to counter or defend against an opponent's offensive strike, while the destruction inherent with the use of nuclear weapons made their contestability impossible.[131] Weapons of the RMA were contestable and introduced an uncertainty that is also characteristic of cyber-weapons. Technologic advances coupled

---

130 Mark Hosenball and Patricia Zangerle, "Cyber-attacks are leading threat against US: spy agencies," *NBC News*. Last modified March 13, 2013, http://www.nbcnews.com/technology/technolog/cyber-attacks-are-leading-threat-against-us-spy-agencies-1C8830308.

131 Paul et al., 309.

with secrecy made it difficult to determine the exact capabilities of the weapons being developed by one's adversary and whether defenses were adequate to counter the weapons. Because RMA weapons employed kinetic means, the realm of possible targets was large, but comprehensible. Continued technologic advances, increased digital connectivity, and substantial secrecy around all aspects of cyber-weapons enhance their contestability, while the abilities to be employed both kinetically and non-kinetically exponentially multiply the number of potential attack surfaces. The ambiguity of this weapon's development and capabilities makes it difficult for a state to determine if it is offensively adequate for the intended purpose or if their defenses are robust enough to protect against the enemy's cyber-weapons.

A final point revealed by the case studies was that a cyber-attack expands the attacking force to anybody sympathetic to adversary's cause. In the Georgian case, attacks were traced to sympathetic hacker citizens in Ukraine and Latvia.[132] Assuming that these attackers are lower-level individuals without access to cyber-tools that can cause catastrophic damage (and thereby invite international scrutiny) their activity on behalf of the aggressing state is almost a no-lose situation. It frees government resources to focus on other aspects of the hostility, but most importantly provides the state with plausible deniability. While the state would have difficulty in controlling some of the more radical hackers, it is safe to assume that they are the minority and that their small numbers prevent them from massing significant effects. The large bot-master command and control servers are likely to be much more accessible to government officials seeking to alter or curb their activity.

B. POLICY CHALLENGES AND RECOMMENDATIONS

The results of this research lead to several policy recommendations that will focus on limiting an adversary's ability to benefit from an offensive cyber-attack. The recommendations focus on defense because it is of critical and immediate importance in order to protect against potential adversaries, and also because the offensive use of weapons is both more intuitive and better-suited for classified research.

132 Tikk et al., *Cyber Attacks Against Georgia,* 14.

The first recommendation is that states need to be held accountable for actions originating from within their borders through updates to applicable international laws. While positively attributing a cyber-attack is difficult, the case studies both revealed circumstantial and tangible evidence that indicated the identity of the aggressor. In addition to inflammatory government rhetoric and Russian attack origins in both case studies, the government of Russia refused to cooperate with an international agreement requiring their cooperation in the Estonian investigation.[133] Allowing Russia to protect the guilty parties, whether it was the actual government or a government-protected entity, without collective international chastisement establishes a dangerous precedent. When there are no consequences for hosting cyber-attacks, then states will continue to hide behind the plausible deniability while secretly manipulating their cyber-forces as desired. The extended routing of data and the ability to launch attacks from remote servers makes it very easy to mask one's identity and certainly complicates any effort to attribute attacks, but if states were held liable for harboring certain types of malicious activity then those states would be forced to become more vigilant. Although forensically more difficult, in theory this is no different than a state harboring terrorists. It should be the responsibility of the state to monitor their networks and prevent promulgation of malicious cyber-attacks. This responsibility is essential to make state governments carefully measure their actions and those within their borders.

The second recommendation calls for an update to international laws and treaties. Perhaps the most significant impediment to the proper prosecution of cyber-attacks is the shortcoming of the international legal framework. Because it was written before cyber-attacks existed, the relevant legal frameworks of international law, international human rights law, and international humanitarian law are fragmented and provide adequate area for adversary states to operate without retribution. Specifically determining when a cyber-attack meets the United Nations (UN) charter criteria for an armed attack and if that attack warrants UN-sanctioned self-defense are two issues that complicate efforts to

133 Ottis, *7th European Conference on Information Warfare*, 3.

effectively deal with cyber-attacks.[134] The difficulty of attribution further complicates a clear delineation between acts of cyber-terrorism, cyber-crime, and cyber-warfare. Had there been internationally agreed-upon standards for the benchmarks of cyber-attacks and the requirements for attribution, the Russian attacks against Estonia and Georgia may have been met with authoritative international counter-action. Establishment of laws that deal specifically with the nuances of the cyber-domain and establish guidelines sufficient to attribute cyber-attacks will create a framework that will better deter an actor's exploitation of cyber-weapons. [135] Hand in hand with an update to the legal framework is the establishment of a representative international body that develops standards for cyber security.[136] Such an organization would allow for pertinent cyber-security issues to be discussed and solutions agreed upon by its member-states.

The third recommendation takes the additional step of arguing for American participation in cyber-treaties that restrict the use of cyber-weapons. So far this issue has been divisive and consequently failed to be implemented. Opponents argue that signing a restrictive arms-control treaty annuls American IT advantages and would prevent exercise of actions critical to national security such as Stuxnet.[137] On the other hand, proponents of establishing treaties contend that cyber-weapons should be viewed as weapons of mass destruction and that increased transparency and voluntary participation in restricting their use is essential to continued security.[138] Much like the transparency of nuclear capabilities during the Cold War created predictable interaction between states proponents argue that the covert and clandestine use development of cyber-weapons as a matter of state policy will foster instability.[139] The recommendation to participate in multilateral international treaties is based on the contention that the devastating effects of

134 Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber-Attacks in International Law," (unpublished paper, Stanford University), 5-6.

135 Shackelford, unpublished paper, 76.

136 Ibid., 73.

137 Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law* 17, no. 2 (2012), 206.

138 Richard Clarke and Robert Knake, *Cyber War* (New York: HarperCollins Publishers (2010), 268.

139 Ibid.

cyber-weapons are so great, particularly when the capabilities are secretly guarded, that collective restriction and enforcement provides the best chance to ensure security among rational actors. Additionally, entering into legal agreements provides a solid base from which to prosecute those who violate it—provided that the transgression can be proved.

The difficulty in attribution leads to the fourth recommendation which is to continue investing in new technology in order to gain and maintain an edge on adversaries. One area for investment is in the field of digital forensics. A nebulous cyber-domain that encompasses rapidly changing technology provides an advantage to those who wish to remain anonymous.[140] In order to overcome the potential advantages gained by non-attributable attacks it is imperative to fund scientific advances in digital forensics. A second area for investment is quantum computing. Quantum computing is nascent technology that will completely revolutionize the landscape of IT. It has the power to negate all current cryptography and make code-breaking a simple process. Similarly, once quantum computing is used to protect a system then current methods of hacking are rendered useless. Russia, China, and the United States are competing to harness this technology into a usable form, and needless to say the winner will gain a remarkable advantage over adversaries.[141] The United States is currently losing over $13 billion annually to cyber-espionage and theft, much of which is reportedly orchestrated by the Chinese government, to adversaries using traditional methods of defeating

---

[140] Tamer Gayed, "Cyber Forensics: Representing and (Im)proving the Chain of Custody Using the Semantic Web, The Fourth International Conference on Advanced Cognitive Technologies and Applications," *COGNITIVE 2012 : The Fourth International Conference on Advanced Cognitive Technologies and Applications*, (2012), 20.

[141] Ben Ionnatta, "Quantum Computing Could Bust Secret Codes—Someday," *Defense News*, last modified November 8, 2012. http://www.defensenews.com/article/20121108/C4ISR01/311080006/Quantum-Computing-Could-Bust-Secret-Codes-8212-Someday

cryptography.[142], [143] It is likely that this financial loss would pale in comparison to the financial damage that adversaries could cause using quantum computing. For this reason, quantum computing technology is a second area that should continue to receive substantial government support.

The final recommendation deals with the establishment of adequate cyber-security defenses. While the government is responsible for protecting its own cyber-assets, the private sector is left largely unregulated to defend itself. This is a problem because the private sector controls a substantial amount of critical infrastructure and is also heavily involved in national and cyber-security contracts, production, and maintenance. Some advocate providing incentives for businesses to meet cyber-security standards instead of mandating compliance, but this approach is insufficient.[144] The government needs to establish and enforce higher cyber-security standards in the private sector in order to stop the outpouring of money and information critical to national security. While serving as a special adviser to the White House regarding cyber-affairs in the early 2000s, Richard Clarke recommended the establishment of cyber-security regulations for the private sector, but was reportedly ignored in fear of the financial and political backlash from big businesses.[145] Perhaps a mixture of incentive and regulation is the best way for both government and the private sector to have ownership of cyber-security, but what is becoming more apparent is that the current solution to private sector cyber-security is inadequate and jeopardizes American national interests.

---

142 FBI News Blog, "FBI Updates Congress on Threats Involving Insiders," last modified June, 28, 2012. http://www.fbi.gov/news/news_blog/fbi-updates-congress-on-threats-involving-insiders-illegal-transfer-of-u.s.-technology

143 Mike Rogers, Statement to the U.S. House, Permanent Select Committee on Intelligence, *Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation*, Hearing, October 4, 2011, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf, accessed March 13, 2013.

144 O'Connell, *Journal of Conflict and Security Law*, 208.

145 Amitai Etzioni, "Cybersecurity in the Private Sector", *Issues in Science and Technology* 28, no. 1 (2011): 60.

C. RECOMMENDATIONS FOR FURTHER RESEARCH

The assumptions for interactions between states were based upon traditional realist theory, particularly those proposed by Waltz and Fearon. This analysis assumed that the actors were rational and either risk-neutral or risk-averse. While this framework accurately describes the interaction of most of the international community, there are states whose actions do not follow the tenets of traditional realism. There is certainly a need for exploratory research regarding the potential use of cyber-weapons by states or groups that are neither risk-neutral nor realist. While the lack of empirical evidence makes it difficult to draw fact-supported conclusions, this research is a valid thought experiment that could produce recommendations for policy-makers and security experts on how to defend against these actors.

In order to best determine the role that the proposed causal variables had on the level of effectiveness it was necessary to select case studies of similar intent. This had the obvious impact of limiting the number of case studies available, but also limited the applicability of the conclusions. There is opportunity for further research to select case studies with a different intent than attacks on availability of data in order to subvert the government's ability to provide services to its people. Cases where cyber-attacks attempt to affect the integrity of data, for either destructive or non-destructive purposes, are some examples of different intents.

There is opportunity to examine the Estonian and Georgian case studies again with the same intent while proposing different causal variables. That research would help to provide a more robust assessment of the exact mechanics of each case study. Because of the secrecy involved with the specifics of cyber-weapons and cyber-attacks, it is difficult to draw definitive conclusions when examining only selected causal variables. In an effort to protect plausible deniability, states are sometimes forced to act in a manner that makes it difficult to determine if certain effects are intended or unintended. It is possible that the role of a proposed variable in the resulting level of effectiveness of an attack has been improperly ascribed. An investigation of all causal variables would help to shed light on all aspects of the case study and better determine the role each played. Unfortunately time prevented an examination of this rigor.

The research conducted in this thesis was mainly qualitative due to the lack of quantitative data available on the specifics of the attack. It also became apparent there is not a commonly used quantitative metric that sheds light on a state's vulnerability to cyber-attack. Organizations such as the World Bank publish an annual report that details the Internet's penetration rate among the population, but there is not a definitive way to determine the approximate vulnerability of a state.[146] To do so would likely require at least an analysis of the target state's digital assets, the difficulty in introducing a cyber-weapon to affect those assets, and the sufficiency of their defense measures. While determining the specific cyber-vulnerability of a state is likely impossible, the fields of modeling and simulation could be very useful in assessing weaknesses and providing decision-makers with better metrics than Internet penetration rates.

A final suggested area for future research is to explore the ramifications of a declaratory retaliation policy. The development of second-strike nuclear capability and policy in retaliation for a first-strike nuclear attack was the significant foundation of strategic deterrence theory during the Cold War.[147]Rapid and clandestine development of cyber-weapons coupled with the additional complexities introduced by nebulous international opinion on how to enforce cyber-security make this topic worth investigating. By creating a red-line that evokes retaliation when crossed by a cyber-attack, the intent is to deter the use of first-strike cyber-attacks. Some of the issues to consider when examining this policy are whether retaliation should be in-kind, the appropriate level of response for a given cyber-attack, and how to proceed when attribution is not concrete.

---

[146] The World Bank, Internet Users (per 100 people).

[147] Dmitri Alperovitch, "Towards Establishment of Cyberspace Deterrence Strategy," *3rd International Conference on Cyber Conflict*, (2011): 2.

LIST OF REFERENCES

African Network Information Center. “Estonia Cyber Attacks 2007.” Accessed December 14, 2012. http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.

Armed Forces Communications and Electronics Association. “The Russo-Georgian War 2008: The Role of Cyber Attacks in the Conflict.” May 24, 2012, accessed January 25, 2013. http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Art, Robert. “To What Ends Military Power?.” *International Security* 4, no. 4 (1980): 3–35.

Blanken, Leo. *Fearon and the Puzzle of Conflict: Unitary Rational Actors Choosing War*. Classroom slideshow. Accessed November 20, 2012. https://cle.nps.edu/xsl-portal/site/3b74a4a9–2968–4d06–8c54-cc0643ec9c61/page/1025a83a-f0ee-4015–8938–16d32223dbb1.

Brodie, Bernard. *Strategy in the Missile Age*. Santa Monica, CA: The RAND Corporation, 1959.

Bumgarner, John, and Scott Borg. *Overview by the U.S.-CCU of the Cyber Campaign Against Georgia in August of 2008*. Special report. Boston: United States Cyber Consequences Unit, 2009.

Central Intelligence Agency. “1992 World Factbook: Estonia.” Accessed December 14, 2012. http://nodedge.com/ciawfb/.

Council on Foreign Relations, “Loose Nukes,” January 2006, accessed December 2, 2012. http://www.cfr.org/weapons-of-terrorism/loose-nukes/p9549.

Czosseck, Christian, Rain Ottis, and Anna-Maria Taliharm. “Estonia After the 2007 Cyber Attacks: Legal, Strategic, and Organisational Changes in Cyber Security.” In *The Proceedings of the 10th European Conference on Information Warfare and Security*. Academic Publications, 2011.

Estonian Information System’s Authority. “Facts about Estonia.” Accessed December 14, 2012. https://www.ria.ee/facts-about-e-estonia/.

Etzioni, Amitai. “Cybersecurity in the Private Sector.” Issues in Science and Technology 28, no. 1 (2011): 58–62.

Fearon, James. “Rationalist Explanations for War,” *International Organization* 49, no. 3 (1995): 379–414.

Federal Bureau of Investigation News Blog. “FBI Updates Congress on Threats Involving Insiders.” Last modified June, 28, 2012. http://www.fbi.gov/news/news_blog/fbi-updates-congress-on-threats-involving-insiders-illegal-transfer-of-u.s.-technology.

Federation of American Scientists. “Status of World Nuclear Forces.” Accessed December 2, 2012. http://www.fas.org/programs/ssp/nukes/nuclearweapons/nukestatus.html.

Foltz, Andrew. “Stuxnet, Schmitt Analysis, and the Cyber ‘Use of Force’ Debate.” *Joint Force Quarterly* 67, no. 4 (2012): 40–48.

Gayed, Tamer. “Cyber Forensics: Representing and (Im)proving the Chain of Custody Using the Semantic Web, The Fourth International Conference on Advanced Cognitive Technologies and Applications.” *COGNITIVE 2012 : The Fourth International Conference on Advanced Cognitive Technologies and Applications*, 2012.

Geers, Kenneth. “Cyberspace and the Changing Nature of Warfare.” *Cooperative Cyber Defense Center of Excellence*. Accessed December 16, 2012. http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf.

George, Alexander. *The Limits of Coercive Diplomacy*. Boulder, CO: Westview Press, 1994.

George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. MIT Press: Cambridge, MA: 2005.

Goertz, Gary. *Social Science Concepts: A User’s Guide*. Princeton: Princeton University Press, 2006.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

Hosenball, Mark, and Patricia Zangerle. “Cyber-attacks are leading threat against U.S.: spy agencies.” *NBC News*. Last modified March 13, 2013. http://www.nbcnews.com/technology/technolog/cyber-attacks-are-leading-threat-against-us-spy-agencies-1C8830308.

Ionnatta, Ben. “Quantum Computing Could Bust Secret Codes—Someday.” *Defense News*. Last modified November 8, 2012. http://www.defensenews.com/article/20121108/C4ISR01/311080006/Quantum-Computing-Could-Bust-Secret-Codes-8212-Someday.

Jervis, Robert. “Introduction: Approach and Assumptions.” In *Psychology and Deterrence*. Robert Jervis, Ned Lebow, and Janice Stein eds. Baltimore: Johns Hopkins Press, 1985.

Kaplan, Fred. *The Wizards of Armageddon*. New York: Simon & Schuster, 1983.

Kitman, Jamie. “President Ilves: The Man Who Made E-stonia.” *The Guardian*. November 3, 2011, accessed December 14, 2012. http://www.guardian.co.uk/world/2011/nov/03/president-ilves-made-estonia.

Libicki, Martin. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009.

Mearsheimer, John. “The False Promise of International Institutions.” *International Security* 19, no. 3 (1994): 5–49.

Nazario, Jose. “Politically Motivated Denial of Service Attacks.” In *The Virtual Battlefield: Perspectives on Cyber Warfare*. Christian Czosseck and Kenneth Geers eds. Washington, DC: IOS Press, 2009.

O’Connell, Mary Ellen. “Cyber Security without Cyber War.” Journal of Conflict and Security Law 17, no. 2 (2012):187–209.

Ottis, Rain. “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.” *Proceedings of the 7th European Conference on Information Warfare*. Academic Conferences Limited ,2008.

Paul, T. V., Patrick Morgan, and James Wirtz, eds. *Complex Deterrence: Strategy in the Global Age*. Chicago: University of Chicago Press, 2009.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

Schelling, Thomas. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Shackelford, Scott. “Estonia Three Years Later.” *Journal of Internet Law* 8, no. 13 (2010): 22–29.

———. “From Nuclear War to Net War: Analogizing Cyber-Attacks in International Law.” Unpublished papers, Stanford University, 2008.

Stiennon, Richard. *Surviving Cyber War*. Lanham, MD: Government Institutes, 2010.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri,Mari Kert, Anna-Maria Talihärm, and Liis Vihul. Cyber Attacks Against Georgia: Legal Lessons Identified. Special report. Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2008.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian*. May 16, 2007, accessed December 14, 2012. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Waltz, Kenneth. *Theory of International Politics.* Random House: New York, 1979.

World Bank. “Internet Users (per 100 people): 2007.” Accessed January 12, 2012. http://data.worldbank.org/indicator/IT.NET.USER.P2?page=1.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr Dan Boger
   Naval Postgraduate School
   Monterey, California